CID REGULATION 195-1

CRIMINAL INVESTIGATION

OPERATIONAL PROCEDURES

U.S. ARMY CRIMINAL INVESTIGATION COMMAND
15 June 2004
(Version 2)

TABLE OF CONTENTS

COVER	Book Cover
TITLE PAGE	Title Page
DISTRIBUTION	Distribution
GLOSSARY	Abbreviations and Acronyms Terms Definitions
CHAPTER 1:	**General Information**
Section I General	
1-1	Purpose
1-2	Policies
1-3	Overseas operations
1-4	Exceptions to policy
CHAPTER 2:	**USACIDC Authority and Responsibility**
Section I General	
2-1	General
2-2	Authority within the United States
2-3	Authority outside the United States
2-4	Determination and acceptance of responsibility
2-5	Assumption of responsibility by higher headquarters
2-6	Investigations involving Army Reserve components
2-7	Investigations involving Army National Guard
2-8	Violations by U.S. Army Recruiting Command (USAREC) personn
2-9	Investigations involving the U.S. Army Corps of Engineers (USACE
CHAPTER 3:	**Special Agents**
Section I Authority	
3-1	Authority
3-2	Authority to administer oaths
3-3	Civilian special agents
3-4	Authority to apprehend/detain
3-5	Authority to search and seize/serve warrants of attachment
3-6	Authority to use and bear arms
3-7	Pursuit Driving
Section II Covert Operations	
3-8	Prior approval required
3-9	Assumed military role

3-10 Obtaining identification cards and ration control documents for covert special agents
3-11 Obtaining operational nicknames

Section III Dress and Disclosure of Grade
3-12 Civilian clothing and non-standard appearance
3-13 Military clothing
3-14 Disclosure of grade

Section IV Billeting, Travel and Conduct
3-15 Billets and messes
3-16 Freedom of movement
3-17 Safeguarding weapons and equipment during travel
3-18 Standards of conduct

CHAPTER 4: Administration of Investigations

Section I General
4-1 Purpose
4-2 Scope
4-3 Extent
4-4 Limitation of investigative effort

Section II Receipt and Development of Complaints
4-5 Receipt and development of complaints
4-6 Monitorship of investigations

Section III Preliminary Investigations and Initiation of Criminal Investigations
4-7 Purpose and procedures of preliminary investigations
4-8 Results of preliminary investigations
4-9 Procedures for criminal investigations

Section IV Referred, Joint, and Collateral Criminal Investigations
4-10 Referral of investigation
4-11 Classified or sensitive programs
4-12 Joint investigations
4-13 Collateral investigations
4-14 Coordination of investigations with the FBI
4-15 Documentation of Department of Justice declination to prosecute

Section V Termination of Investigations

4-16	Early/immediate case closure
4-17	Termination of Reports of Investigations (ROI)

Section VI Military Police Reports

4-18	Preparation
4-19	USACIDC use

Section VII Special Considerations

4-20	Fugitive deserter ROI
4-21	Evidence in a fugitive deserter ROI
4-22	Return of fugitive deserters to U.S. Army control
4-23	Reopening Final (D) ROI
4-24	ROI involving units participating in selected field training exercises (FTXs) and contingency operations
4-25	Sensitive investigations
4-26	Inspector General reports
4-27	Requests for information/records from the National Personnel Records Center
4-28	Criminal investigative support for suspension and debarment
4-29	Violations by USAREC personnel
4-30	Violations by health care providers
4-31	Internal Revenue Service (IRS)
4-32	Military Intelligence (MI) coordination
4-33	United States Secret Service (USSS)
4-34	Support by United States Marshals Service (USMS)
4-35	Postal investigations
4-36	Investigative support to Defense Protective Service (DPS)
4-37	Centralized Accident Investigation Ground (CAIG) program
4-38	The Defense Investigative Management Information System (DIMIS)
4-39	Reporting of significant economic crime (EC) cases
4-40	Initiation of ROIs in Deployment Situations
4-42	Processing of USAR Personnel for Positive Urinalysis Results
4-43	Procedures involving incidents of obtaining services (telephone services) under false pretenses
4-44	Intelligence Related Investigations
4-45	U.S. Soldiers' and Airmen's Home
4-46	Hate Crimes Investigations

CHAPTER 5:	**Conduct of Criminal Investigations**

Section I Conduct of Criminal Investigations

5-1	Interviews
5-2	Interrogations
5-3	Interrogation Procedures
5-4	Special interviews/interrogations
5-5	Victim/witness assistance
5-6	Written statements
5-7	Verbal statements
5-8	Certificates
5-9	Medical records/medical information
5-10	Photography/photocopied evidence
5-11	Crime scene and evidence processing
5-12	Photographing persons
5-13	Fingerprinting persons
5-14	Submission of fingerprint cards (FD-249/R-84) to the FBI
5-15	Identification photograph files (mug files)
5-16	Line-ups
5-17	CID wanted poster
5-18	Controlled substances
5-19	Bomb threats
5-20	Hostage situations
5-21	Death investigations
5-22	Missing persons
5-23	Reporting of casualties during operations other than war
5-24	Supervisory considerations for death investigations
5-25	Adult private consensual sexual misconduct
5-26	Self-confessed offenders
5-27	Terrorism and major disruption
5-28	U.S. Government owned weapons
5-29	Coordination with Staff Judge Advocate (SJA)
5-30	Provost marshal coordination
5-31	Other coordination
5-32	Briefing installation commanders and senior personnel

Section II Special Investigative Assistance

5-33	General
5-34	Polygraph
5-35	Intercept of wire and oral communications for law enforcement purposes
5-36	National Crime Information Center (NCIC)
5-37	USACRC records checks
5-38	FBI records checks

5-39 The Violent Criminal Apprehension Program (VICAP)

Section III Authorizations, Warrants, Complaints, Subpoenas and Summonses
5-40 Military
5-41 Federal
5-42 Other civilian warrants
5-43 Financial records of private persons
5-44 Obtaining information from the U.S. Customs Service on monetary transactions under the Bank Secrecy Act

Section IV Federal Grand Jury Proceedings
5-45 General
5-46 Grand jury functions
5-47 Matters occurring before the grand jury
5-48 Use of grand jury material in civil proceedings
5-49 Access list
5-50 Security and accountability of grand jury materials
5-51 Grand jury subpoenas
5-52 Transmission of grand jury material
5-53 Grand jury material in reports of investigation
5-54 Storage at Crime Records Center
5-55 Disposition of grand jury material

Section V Release of Information
5-56 Media relations
5-57 Public Website Administration
5-58 Public Appearances and Presentation by USACIDC Personnel
5-59 Procedures for release of information

Section VI Risk Management
5-60 General
5-61 Objectives
5-62 Approval levels
5-63 Reducing risk levels
5-64 Case file documentation

Section VII Violation of Rules of Engagement by USACIDC Personnel During Operations Other than War
5-65 General

Section VIII Cooperation with Civilian Law Enforcement Officials (CLEO) Reports
5-66 General

CHAPTER 6:	ROI Management/Management Control
Section I Documentation and Control Numbers	
6-1	Documentation
6-2	Sequence numbers
6-3	Report of Investigation (ROI) numbers
6-4	Offense code
Section II CID Action Record	
6-5	Requirement
6-6	Preparation
6-7	Use
6-8	Completion
Section III CID Case Folder	
6-9	Requirement
6-10	Filing
6-11	Preparation
6-12	Release of case folder
6-13	Case file storage
Section IV Consolidated Complaint/Case Log	
6-14	Purpose
6-15	Requirement
6-16	Preparation
Section V ROI Management	
6-17	General
6-18	Case status board
6-19	Investigative plans
6-20	Case review
6-21	Quality control procedures
Section VI Management Control	
6-22	Law Enforcement Availability Pay (LEAP)
6-23	Sex Crimes/Child Abuse Monitorship

CHAPTER 7:	Investigative Reports

Section I General

7-1	Purpose
7-2	Classification of USACIDC reports
7-3	Preparation

Section II Categorization of Subjects, Victims, Investigations, and Offenses

7-4	Subjects
7-5	Victims
7-6	Investigations and offenses
7-7	Exceptions
7-8	Lesser related offenses
7-9	Lesser related offenses perpetrated by a listed subject

Section III Serious or Sensitive Incident (SSI) Reports

7-10	SSI reporting criteria
7-11	SSI preparation and dispatch

Section IV Types of Investigative Reports

7-12	Initial ROI
7-13	Status ROI
7-14	Final ROI
7-15	Initial/Final ROI
7-16	Interim ROI
7-17	Supplemental ROI
7-18	Reopened investigations
7-19	Corrected ROI
7-20	Referred ROI
7-21	Collateral ROI
7-22	Joint ROI

Section V Agent's Investigative Report (AIR)

7-23	Purpose
7-24	Preparation

Section VI Internal USACIDC Reports

7-25	Request for assistance (RFA)
7-26	Information report
7-27	Agent's Activity Summary (AAS), CID Form 28
7-28	Interview worksheet (CID Form 44)

7-29 Crime Records Data Reference Card (DA Form 2804)
7-30 Criminal Intelligence Report (CID Form 97)
7-31 Document Cover Sheet (CID Form 14)
7-32 Commander’s Report of Disciplinary or Administrative Action Take (DA Form 4833)
7-33 Workload (work-hour) reporting

Section VII Figures
7-1 Initial Report Format
7-2 Status Report Format
7-3 Final Report Format
7-4 Interim Report Memorandum
7-5 1st Supplemental Report Format
7-6 2nd Supplemental Report Format
7-7 Agent's Investigative Report (Non-Form)
7-8 Agent's Investigative Report (Form)
7-9 Agent's Investigative Report (Form)
7-10 Agent's Activity Summary
7-11 Internal USACIDC Memorandum for Record
7-12 CID Form 14, Document Cover Sheet
7-13 DA Form 4833, Commander's Report of Disciplinary or Administrative Action
7-14 Action Commander's Memorandum of Transmittal (MOT)
7-15 Initial/Final ROI

CHAPTER 8: Distribution

Section I General
8-1 General
8-2 Variances

Section II Routine Distribution of ROI
8-3 General
8-4 Original
8-5 File copy
8-6 Intermediate USACIDC headquarters
8-7 Other USACIDC elements
8-8 Provost marshal

Section III Identified Subject
8-9 General
8-10 Supported commander/supervisor

8-11	Staff judge advocate (SJA)
8-12	USAREC LNO
8-13	Transients
8-14	Fugitive deserters

Section IV Additional Distribution of Final, Collateral and Supplemental ROI

8-15	Death investigations
8-16	Overseas support to U.S. Department of Justice (DOJ)
8-17	Postal offenses
8-18	Internal Revenue Service (IRS)
8-19	Counterfeit U.S. currency
8-20	Appropriated funds
8-21	U.S. Army commissaries
8-22	Non-appropriated funds
8-23	Child sexual abuse in DoD-sanctioned activities
8-24	Department of Defense Education Activity (DoDEA)
8-25	Significant cases of fraud and corruption
8-26	Depot Systems Command (DESCOM)
8-27	Defense Logistics Agency (DLA)
8-28	Army and Air Force Exchange Service (AAFES)
8-29	U.S. Army Corps of Engineers (USACE)
8-30	U.S. Army Materiel Command (AMC)
8-31	U.S. Army Information Systems Command (ISC)
8-32	Military Traffic Management Command (MTMC)
8-33	U.S. Army Space and Missile Defense Command (USASMDC)
8-34	U.S. Army Space Command (ARSPACE)
8-35	ROIs involving U.S. Army museums
8-36	Offenses by commercial agents
8-37	Military Prisoner Transfer and Assignment Criteria to the Army Correctional System
8-38	Defense Intelligence Agency

Section V Serious or Sensitive Incident (SSI) Reports

8-39	SSI Only
8-40	ROI/SSI

Section VI Sensitive Information

8-41	General
8-42	Senior personnel
8-43	Compromise of investigative effort
8-44	Classified and sensitive programs

Section VII Distribution of Crime Prevention Survey Reports (CPS)
8-45 Normal distribution
8-46 CPS reports distributed outside of USACIDC
8-47 Intelligence-related Investigations

CHAPTER 9: Relationships Between CID and Military Police (MP)

Section I General
9-1 Cooperation
9-2 Working relationship and supervision
9-3 Control in investigative situations
9-4 Investigative activities of the CID and MP
9-5 Memorandum of understanding (MOU)
9-6 Investigative assistance
9-7 Training
9-8 Criminal intelligence
9-9 Controlled substances
9-10 Evidence
9-11 Detention
9-12 Drug suppression team (DST) member

CHAPTER 10: Economic Crime Program

Section I Economic Crime Program
10-1 Mission
10-2 DoD policies concerning economic crime investigations
10-3 Jurisdiction
10-4 Economic crime offenses
10-5 Economic crime investigative responsibilities
10-6 USACIDC management responsibilities
10-7 Economic crime investigative procedures
10-8 Criminal Investigation of Fraud Offenses
10-9 Voluntary Disclosure Program
10-10 Coordination of investigations with the Defense Procurement Frau Unit (DPFU)
10-11 Program Fraud Civil Remedies Act
10-12 Anti-Kickback matters
10-13 Screening of major contract accounting fraud cases
10-14 Screening and review procedures
10-15 Referral to the DOJ or a U.S. Attorney's Office (USAO)
10-16 Reporting of screened cases

Section II Developing and Implementing the Economic Crime Program
10-17 General
10-18 The economic crime threat assessment (ECTA)
10-19 The ECTA process
10-20 Target analysis files (TAF)
10-21 TAF scheduling
10-22 Fraud awareness briefings (FAB)
10-23 Special investigative operations
10-24 LOGSEC operations in support of Army deployments and exercise
10-25 Economic crime reference library

Section III The USACIDC CPS Program
10-26 The Army crime prevention program
10-27 USACIDC CPS Program
10-28 Conducting CPSs of USAR, ROTC and ARNG facilities
10-29 Preparation for conducting the CPS
10-30 Initiation of the CPS
10-31 Entrance briefing
10-32 Investigative activities resulting from the CPS
10-33 Exit briefing
10-34 CPS conducted by CID reserve special agents
10-35 CPS reports
10-36 Preparation of the CPS report
10-37 Reporting results of corrective action
10-38 Supplemental CPS reports
10-39 Follow-up action
10-40 Classification of CPS reports
10-41 Release of information

Section IV Cost Avoidance Reporting in ROIs and CPS Reports
10-42 Cost avoidance computation
10-43 Reporting criminal cost avoidance

Section V Personnel Requirements and Training
10-44 Personnel and training
10-45 Military economic crime supervisors
10-46 Civilian education program

CHAPTER 11: Major Procurement Fraud Investigations

Section I General
11-1 General
11-2 Major Procurement Fraud Unit (MPFU) structure and operations
11-3 Major procurement fraud investigations
11-4 MPFU investigative purview
11-5 MPFU management responsibilities
11-6 MPFU field element operational procedures
11-7 Receipt and development of cases
11-8 MPFU joint investigative procedures
11-9 Financial Crimes Enforcement Network (FinCEN) requests
11-10 Task force operations
11-11 Qui Tam
11-12 Major procurement fraud investigation reports
11-13 U.S. Attorney case presentation

CHAPTER 12: Computer Related Crime

Section I Computer Crime
12-1 Definitions
12-2 General Responsibilities
12-3 Computer Crime Investigations Committee (CCC)
12-4 Specific USACIDC responsibility
12-5 Training
12-6 Investigating computer network intrusions

Section II Other Computer Crime Activity and Operational Guidance
12-7 Investigative activities
12-8 Child Pornography, Adult Pornography and Other Obscene Matter

Section III Figures
12-1 Electronic Crime Vulnerability Assessment (ECVA)
12-2 Computer Intrusion/Incident Checklist and Information Report
12-3 Memorandum for Record (Evaluation of Evidence

CHAPTER 13: Drug Suppression Program

Section I General
13-1 Purpose
13-2 Responsibilities
13-3 Policies
13-4 Objectives

Section II Drug Suppression Operations

13-5	General
13-6	Levels of drug suppression operations
13-7	Organization
13-8	Department of Defense (DoD) affiliation in CONUS and OCONUS
13-9	Drug suppression operations within the territorial jurisdiction of the United States
13-10	Drug suppression operations outside the territorial jurisdiction of the United States
13-11	Military Police drug suppression activities
13-12	USACIDC procedures for monitoring MP drug suppression activities and/or assuming investigative jurisdiction
13-13	Field test analysis of suspected controlled substances
13-14	Investigation of deaths caused by drug overdose
13-15	DoD assistance in drug interdiction and suppression
13-16	Army Substance Abuse Program (ASAP)
13-17	Possession or distribution of controlled substances
13-18	Controlled purchases, confidence buys, and fronting
13-19	Use of controlled substances by special agents and personnel performing drug investigation duties
13-20	Federal agencies involved in drug suppression activities
13-21	Reports
13-22	APO First Class Mail controlled substance seizure investigations (CONUS)
13-23	Security of Army Post Office mail overseas (OCONUS)
13-24	Seizure and forfeiture of vehicles

Section III USACIDC Drug Suppression Drug Survey Program

13-25	General
13-26	Objectives
13-27	Responsibilities
13-28	Execution
13-29	Reporting format
13-30	Reporting requirements

Section IV Working with Other Investigative Agencies

13-31	Coordination
13-32	Responsibilities of federal agencies in drug suppression activities

Section V DoD Directive 5525.7

13-33	Guidance

13-34 Policy
13-35 Approvals
13-36 Coordination
13-37 Request for approval
13-38 After-action reports

Section VI Seizure & Forfeiture of Vehicles
13-39 General
13-40 Authority of the DEA
13-41 Policy

Section VII Figures
13-1 Controlled Substance Conversion Chart
13-2 DST Standing Operating Procedure (Sample)

CHAPTER 14: USACIDC Source Program

Section I General
14-1 Purpose
14-2 Explanation of terms
14-3 Responsibilities

Section II Program Effectiveness
14-4 General
14-5 The USACIDC Source Program
14-6 Planning and goals for source operations
14-7 Information sources
14-8 Recruitment and utilization of registered sources
14-9 Protection of source identity
14-10 Transfer of sources
14-11 Discontinued use of registered sources
14-12 Restrictions governing information collection

Section III Records and File Management
14-13 General
14-14 The USACIDC Central Source Register
14-15 CID element source files
14-16 Source code number
14-17 Source data card

CHAPTER 15:	**Protective Services**
Section I General	
15-1	Purpose
15-2	Definitions
15-3	Authority and responsibility
15-4	Policy
15-5	Support to government agencies
15-6	Selection, training and conduct
15-7	Funding
15-8	Operational reporting
15-9	PSU monthly field agent tasker
15-10	Protective service security control room standing operating procedures
CHAPTER 16:	**Combating Terrorism Program**
Section I General	
16-1	General
16-2	Purpose
16-3	Scope
16-4	U.S. Government and Army Policy for Combating Terrorism (Extracted from AR 525-13)
16-5	The Army Combating Terrorism Program (CBT/T) assigns the following responsibilities to the USACIDC
16-6	Responsibilities
16-7	Investigate terrorist acts
16-8	Provide criminal intelligence related to terrorism
16-9	Provide hostage negotiators
16-10	Conduct Personal Security Vulnerability Assessments (PSVA) on Army leaders
16-11	Personal security for senior Army leaders
16-12	Planning considerations Terrorist Incident Report (TIR) (Extracted from AR 525-13 and modified for USACIDC use)
16-13	Terrorist Threat Report (TTR) (Extracted from AR 525-13 and modified for USACIDC use)
16-14	Terrorist Threat Report (TTR) (Extracted from AR 525-13 and modified for USACIDC use)
CHAPTER 17:	**Carrying, Using, Safeguarding and Qualifying with Weapons**
Section I General	

17-1 Purpose
17-2 Responsibilities

Section II Authorization, Carrying, and Use of Weapons
17-3 Authorization documentation
17-4 Responsibility for establishing procedures for the carrying and use of weapons
17-5 Authorized and prohibited weapons and ammunition
17-6 Policies governing the carrying of weapons
17-7 Policies governing the carrying of weapons on commercial aircraft
17-8 Policies governing the use of weapons

Section III Security of Weapons and Ammunition
17-9 General
17-10 Unit security
17-11 Individual security
17-12 Loss, theft, unlawful disposition or recovery of firearms and ammunition

Section IV Use of Holsters
17-13 Authorization for use
17-14 Exceptions to policy
17-15 Loan of weapons and holsters

Section V Other Equipment
17-16 Oleoresin Capsicum (Pepper) Spray
17-17 Hollow-point Ammunition

Section VI Training and Qualification
17-18 General
17-19 Weapons training
17-20 Weapons qualification and sustainment
17-21 Failure to qualify

CHAPTER 18: Criminal Intelligence Program

Section I General
18-1 Purpose
18-2 Scope
18-3 Objectives
18-4 Policy

18-5 Policy exception
18-6 Responsibilities

Section II Criminal Intelligence Processing and Collection Planning
18-7 General
18-8 Intelligence processing
18-9 Collection planning

Section III Criminal Intelligence Management
18-10 General
18-11 Records management
18-12 Information collection
18-13 Sources of information
18-14 Essential elements of criminal intelligence (EECI)
18-15 Intelligence reporting
18-16 Criminal intelligence bulletin (CIB)

Section IV Automated Criminal Intelligence System
18-17 General
18-18 Automation implementation
18-19 System description

Section V Figures
18-1 Sample of Essential Elements of Criminal Intelligence (EECI)
18-2 Criminal Alert Notice (CAN) Instructions and Sample
18-3 Criminal Intelligence Report (CIR) Instructions and Format
18-4 Criminal Intelligence Bulletin (CIB) Format

CHAPTER 19: Process for Acceptance and Accreditation of USACIDC Investigative Personnel

Section I General
19-1 Purpose
19-2 Applicability

Section II Application Process
19-3 Application Process for Military Investigators
19-4 Application Process for Warrant Officer Appointment
19-5 Application Process for Civilian Investigator
19-6 Forwarding Applications
19-7 Actions on Applications

Section III Probationary Period
19-8 Probationary Period

Section IV Request for Return to Active Duty as a CID Agent
19-9 Request for Return to Active Duty as a CID Agent

Section V Release Process
19-10 Release Process

Section VI Accreditation Review Procedures & Administration of the Criminal Investigation Accreditation File (CIAF)
19-11 Administration of the CIAF
19-12 Custodian of the CIAF
19-13 Control of the CIAF
19-14 Access to and loan of the CIAF
19-15 Initiation of the CIAF
19-16 Use of the CIAF
19-17 Documents authorized in the CIAF
19-18 Forwarding of documents for inclusion in the CIAF
19-19 Processing local or general memoranda
19-20 Record access procedures
19-21 Challenging record contents

Section VII Figures
Fig 19-1 Realities of the Investigative Profession
Fig 19-2 CID Application Checklist
Fig 19-3 Authorization for Release of Information
Fig 19-4 Application Cover Memorandum
Fig 19-5 Applicant Background Questionnaire
Fig 19-6 Applicant Financial Questionnaire
Fig 19-7 Disclosure Form
Fig 19-8 Results of Medical Records Screening
Fig 19-9 SAC interview Checklist and Memorandum
Fig 19-10 Termination of Probation
Fig 19-11 Statement of Interview
Fig 19-12 Interview Checklist

CHAPTER 20: USACIDC Intern Training Program

Section I General
20-1 Purpose

20-2 Applicability
20-3 Applicant Eligibility/Acceptance
20-4 Applicant Attachment
20-5 Applicant Training
20-6 Operational Restrictions for Interns.
20-7 Documentation of Training.

Section II Figures
Figure 20-2 CID Intern Declaration of Understanding
Figure 20-3 Completion of CID Intern Training Program

CHAPTER 21 Investigation and Released Process for USACIDC Investigativ and Laboratory Personnel

Section I General
21-1 Purpose
21-2 Policies
21-3 Responsibilities
21-4 Standards

Section II Voluntary Release Pro
21-5 Policy
21-6 Procedure

Section III Involuntary Release Procedures
21-7 Investigations
21-8 Commander's Action
21-9 Action Concerning Commander's Recommendation

Section IV ARB Procedures
21-10 Composition of ARB
21-11 Duties of the President of the ARB
21-12 Conduct of Proceedings
21-13 Conclusion of ARB Proceedings
21-14 Report of Proceedings
21-15 Final Action
21-16 Reclassification Process

Section V Figures
Fig 21-1 Example of an Appointment of Investigating Officer Memorandum
Fig 21-2 Preparing a Memorandum for Inquiry (Format)

Fig 21-3	Notice of Recommended Elimination
Fig 21-4	Notice of Elimination from the CID Program
Fig 21-5	Example of Probationary Report
Fig 21-6(a)	Preparing a Memorandum for Counseling, Admonition, Censure ar Reprimand (Format, First Page)
Fig 21-6(b)	Preparing a Memorandum for Counseling, Admonition, Censure ar Reprimand (Acknowledgement Format, Second Page)

CHAPTER 22:	**CID Credentials, Identification Cards, Badges, Laboratory and Polygraph Certificates**
Section I General	
22-1	Purpose
22-2	Explanation of terms
22-3	Objectives
22-4	Responsibilities
Section II Issue, Eligibility and Procedures	
22-5	Issue of CID agent badges and credentials
22-6	Issue of the CID special agent oath
22-7	Issue of the supervisor badge and credentials
22-8	Issue of the laboratory examiner badge and credentials
22-9	Issue of the indigenous personnel identification card
22-10	Issue of the laboratory examiner certificates
22-11	Issue of the polygraph certificate
22 12	Issue of the CID staff badge and credentials
22-13	Issue of the CID generic credentials
22-14	Issue of CID personnel sequence number
Section III Controls	
22-15	Controls
22-16	Loss, damage, or retirement
22-17	Badge and credentials holder
22-18	Use and Display of CID Badge and Credentials
Section IV Figures	
22-1	Request for Issue of Supervisor Badge and Credentials
22-2	Request for Laboratory Badge and Credentials
22-3	Request for Polygraph Certification
22-4	Request for CID Staff Credentials
22-5	Sample Credential Photos

CHAPTER 23:	**Criminalistics Program**
Section I General	
23-1	Scope
23-2	Program objective
23-3	Responsibilities
Section II The Criminalistics Program	
23-4	General
23-5	Personnel and training
23-6	Equipment approvals
23-7	Funding
23-8	USACIDC criminalistics committee
Section III Procedures	
23-9	General
23-10	Operational and training support
23-11	Equipment acquisition and maintenance
23-12	Development of new investigative techniques
Section IV Figures	
Figure 23-1	Use Guide
CHAPTER 24:	**Forensic Science Officer Program**
Section I General	
24-1	Scope
24-2	Program Objectives
24-3	Personnel, training and utilization
24-4	Responsibilities
CHAPTER 25:	**U.S. Army Crime Records Center: Records, Files and Freedom of Information/Privacy Act Functions**
Section I General	
25-1	Purpose
25-2	Policy
25-3	Responsibilities
25-4	Exceptions to policy

Section II Management
25-5 General
25-6 Information disclosure accounting by USACIDC field elements
25-7 Allocation of case numbers
25-8 Accountability of reports of investigation
25-9 Liaison activities

Section III Records Checks and File Procurement
25-10 General
25-11 Immediate action records/name checks
25-12 Identification index
25-13 Routine records/name checks
25-14 Records checks in support of the U.S. Total Army Personnel Command (TAPC) activities, General Officers Management Office (GOMO), and Senior Executive Service (SES) personnel screenings
25-15 Procurement of files
25-16 Intelligence files procurement
25-17 Use of the National Crime Information Center (NCIC)
25-18 Computerized Criminal Histories (CCH)

Section IV The "CID Wanted" Deserter System
25-19 General
25-20 Crime Records Center procedures

Section V Referral of Criminal History Information Received from Other Investigative Agencies
25-21 General
25-22 Purpose
25-23 Procedures

Section VI Defense Clearance and Investigations Index
25-24 General
25-25 Concept
25-26 Control
25-27 Responsibilities
25-28 DCII insertion/deletion procedures
25-29 Release of information

Section VII Freedom of Information Act (FOIA) and Privacy Act (PA) Program
25-30 General
25-31 Policies

25-32 Control
25-33 Responsibilities
25-34 Procedures

CHAPTER 26: United States Army Criminal Investigation Laboratory (USACIL) Operation

Section I General
26-1 Purpose
26-2 Organization and Mission
26-3 Responsibilities

Section II Policies and Procedures
26-4 General policy of operation
26-5 Procedures for requesting support
26-6 Evidence Submission Requirements
26-7 Examiner accessions, training, and utilizations

Section III Internal Controls
26-8 General
26-9 Areas of internal control

CHAPTER 27: Verification of Information Acquired and Stored Pursuant to USACIDC Criminal Investigative Effort (Temporary Placement)

Section I General
27-1 Purpose
27-2 Applicability
27-3 Policy
27-4 General
27-5 Verification
27-6 Report of prohibited information
27-7 Consolidated report of inspection, Report Control Symbol (RCS) DD-A(A)-1118
27-8 Responsibilities

APPENDIXES

A. Criminal Offense Codes
B. Major Command Assignment Codes (MCAC)
C. Hypnosis Policy
D. Criminal Investigation Standards
E. Liaison Program
F. Cooperation with Civilian Law Enforcement Officials (CLEO) Reports
G. DoD Hotline Program
H. U.S. Army Audit Agency
I. Defense Contract Audit Agency
J. Presentations to Prosecutors
K. Subpoena Documentation
L. Suggested Guide for Preparing a MOU for Drug Suppression Operations
M. A Guide to Source Handling
N. Control Room Standard Operating Procedures
O. Preparation of FD Form 249 and FBI/DOJ Form R-84 (Final Disposition Report)
P. Daytime Practical Pistol Qualification Course
Q. Nighttime Practical Pistol Sustainment Course
R. Range Operations and Safety
S. Internal and External Sources
T. Crime Analysis
U. Reference Publications

CHAPTER 1

Section I General

1-1
Purpose

This regulation is a complete revision of CID Regulation 195-1 and changes are made throughout. It prescribes policies, procedures and responsibilities for the conduct of CID investigative/non-investigative activities; relationships between CID, military police, and other investigative organizations; and the preparation of investigative records, reports and related forms. This regulation provides only internal USACIDC guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal. The words "his", "he" or "him" when used in this regulation represents both the masculine and feminine genders unless only the feminine gender applies.

1-2
Policies

Department of the Army policies pertaining to USACIDC criminal investigation activities are contained in Army Regulation 195-2. This regulation expands upon those policies where necessary and establishes procedures pertaining to criminal investigative activities, reporting of criminal incidents, support functions, and other USACIDC operations. All USACIDC personnel, regardless of assignment, will be governed by this regulation as it pertains to their USACIDC activities.

1-3
Overseas operations

Outside the United States, the provisions of this regulation may be modified as necessary to bring them into agreement with applicable status of forces or similar agreements, the policies of the United States Ambassador, and the desires of the host government. All modifications will be approved by the Commander, USACIDC, prior to implementation. Modification requests will be forwarded through command channels to the Commander, USACIDC, ATTN: CIOP-COP-PO.

1-4
Exceptions to policy

Requests for exceptions from the provisions of this regulation will be forwarded through channels to Commander, USACIDC, ATTN: CIOP-COP-PO, Fort Belvoir, VA 22060.

CHAPTER 2

2-1
General

a. As used in this regulation, authority to investigate refers to the ability to conduct investigative activity without being in violation of law or DoD and Army directives. Responsibility to investigate refers to a requirement to undertake or ensure the conduct of investigative activity. There are numerous instances in which USACIDC has the authority to investigate but does not have responsibility (e.g., most military connected misdemeanors). There can never be responsibility to investigate where authority is lacking. Basic USACIDC investigative authorities and responsibilities are specified in AR 195-2. In determining whether or not to initiate an investigation, it first must be determined that the USACIDC is authorized to conduct the investigation. If so, it must then be determined whether the USACIDC should accept the responsibility for the investigation.

b. The list of offenses at appendix B, AR 195-2, is related to the punitive articles of the Uniform Code of Military Justice (UCMJ). This is not intended to indicate that the USACIDC is responsible for investigating only offenses punishable under the UCMJ.

c. Investigative authority and responsibility of USACIDC for fraud offenses occurring within the DoD are governed by DoD Instruction 5505.2, and implementing instructions.

d. Investigative authority and responsibility of USACIDC concerning activities and personnel of the Army and Air Force Exchange Service (AAFES) are governed by the provisions of AR 19-57.

2-2
Authority within the United States

a. The USACIDC special agents are authorized to investigate any alleged criminal conduct in which there is an Army interest unless prohibited by law or higher authority.

b. Reasonable preliminary investigation may be made to determine if an Army interest exists. Such an investigation, by its nature, accomplishes an Army purpose and is not a violation of the Posse Comitatus Act, 18 USC, 1385.

c. The Posse Comitatus Act prohibits the use of Army elements, including the USACIDC, its agents and sources by civilian law enforcement authorities in the enforcement of civilian laws. However, this prohibition does not prevent USACIDC investigative activity, even when there is civilian law enforcement interest or involvement in the investigation, so long as the reason for the

USACIDC investigation is to satisfy Army investigative needs in a criminal matter of Army interest. The probable disposition of the offender(s), civilian or military, is not a determining factor. The Army interest must be a direct interest, must exist at the time of the USACIDC action, and must be reasonably connected with the USACIDC action taken. The fact that there previously was, or in the future may be, an Army interest is not sufficient. A determination that there is an Army interest must be based upon all the information available at the time and may change upon receipt of further information.

d. Without a prior written request and approval as outlined in paragraph 2-2e, CID field investigative units will not expand their law enforcement authority by seeking deputized state and/or local law enforcement authority. One or more of the following circumstances must exist to support justification for requesting deputized state and/or local law enforcement authority:

(1) the ability to perform an essential command law enforcement function within the jurisdiction is significantly hampered by a lack of authority to enforce state or local laws; and

(2) the need for such law enforcement authority cannot be met effectively by assistance from law enforcement agencies with such authority; and

(3) there are adequate internal safeguards and management controls existing to ensure proper exercise of the authority; and

(4) the advantages to possessing the authority can reasonably be expected to exceed the disadvantages likely involved in exercising the authority; and

(5) the authority to use deputation from state and/or local government has been approved by the Under Secretary of Defense (Personnel and Readiness) or the Secretary of a military department or a designee.

e. For CID personnel to use deputized state and/or local law enforcement authority while performing DoD functions, CID commanders must request through command channels approval for CID personnel to use deputized authority. CID units must present written justification in support of the request to HQ, USACIDC ATTN: CIOP-ZA. The written justification should provide all the relevant information including:

(1) a detailed discussion of the issues identified in paragraph 2-2d above; and

(2) the concurrence or non-concurrence, and any comments, of the appropriate U.S. attorney who would handle legal actions arising from the exercise of the deputation authority; and

(3) a written statement from the state and/or local officials issuing the deputation authorization agreeing with the scope of the delegation authority as defined by the district/battalion commander and acknowledging that deputized CID personnel will not comply with any state and/or local requirement that conflicts in any way with federal law or the CID requirements.

2-3
Authority outside the United States

a. The USACIDC investigative authority and investigative responsibility outside the United States are determined by international treaty or agreement (including status of forces agreements), by the policies of the host government, the U.S. ambassador, and AR 195-2.

b. In the absence of such provisions, the following presumptions will apply:

(1) On Army controlled installations, the USACIDC has the authority to investigate alleged crimes.

(2) Outside Army controlled installations, the USACIDC may investigate after coordination with host country authorities.

(3) In a combat environment or deployment, the USACIDC has the authority to investigate alleged crimes involving Army personnel, property affecting the Army mission, and war crimes. Other investigations may be undertaken if requested by the supported commander in support of the overall Army mission.

c. The USACIDC authority in foreign countries where U.S. Forces are not normally stationed.

(1) Each USACIDC major subordinate commanders will issue written guidance prescribing the authority of special agents in each foreign country within their geographic area of responsibility where USACIDC personnel are stationed or frequently visit on investigative missions. This guidance will be coordinated with the appropriate U.S. embassy and should be included in the organization standard operating procedures.

(2) Written guidance governing the authority of special agents in countries visited only infrequently will be provided in an appropriate form on a case-by-case basis. This guidance will also be coordinated as necessary with the proper U .S. embassy. See also paragraph 3-6c.

(3) Matters requiring coordination directly with the Department of State will be referred to Commander, USACIDC, ATTN: CIOP-ZA. Similarly, policies or procedures imposed by a U.S. embassy which seriously impede the investigative

mission will be referred to Commander, USACIDC, ATTN: CIOP-ZA for resolution with the State Department.

2-4
Determination and acceptance of responsibility

Upon the receipt or development by a USACIDC unit of information indicating that a crime may have occurred, the CID supervisor is charged with determining whether the USACIDC should accept investigative responsibility. The CID supervisor may, when appropriate, consult the provost marshal, SJA, or supported commander. The decision to investigate, however, rests with the CID supervisor. This decision must be made in accordance with AR 195-2, and within CONUS, the 1984 Department of Defense/Department of Justice Memorandum of Understanding as implemented by AR 27-10 and DoD Directive 5525.7. Neither response to a crime scene nor the initiation of a preliminary investigation constitutes acceptance of investigative responsibility.

2-5
Assumption of responsibility by higher headquarters

a. Any higher headquarters within the USACIDC may assume investigative responsibility from a subordinate unit.

b. If at the time of assumption of responsibility, an initial report of investigation (ROI) has not been transmitted, the subordinate unit will complete its Automated Criminal Investigative Reporting System (ACIRS) data file, noting the assumption of investigative responsibility by the higher headquarters, and forward the sequence number action to the higher headquarters using a memorandum of transmittal.

c. If an initial ROI has been transmitted prior to the time investigative responsibility is assumed by the higher headquarters, the subordinate unit will transfer the action in accordance with paragraph 6-22.

2-6
Investigations involving Army Reserve components

a. Personnel

(1) Army Reserve personnel on active duty are subject to the provisions of the UCMJ. Incidents involving these personnel will be investigated by the USACIDC in the same manner as those involving active duty Army personnel.

(2) Army Reserve personnel may be involuntarily ordered to active duty for the purpose of Article 32 investigation, trial by court-martial, or non-judicial punishment for offenses committed while serving in an active duty (AD), active duty for training (ADT), annual training (AT), or inactive duty training period. Army Reserve soldiers remain subject to UCMJ jurisdiction for offenses committed while in a Title 10 USC status notwithstanding termination of a period of such duty, provided they have not been discharged from all further military service.

(3) Generally, ROTC cadets performing military training or attending summer camp on military installations are not subject to the UCMJ. The USACIDC will investigate crimes within its purview committed by ROTC cadets while on military reservations in the same manner as for other civilians.

b. Property crimes and loss of appropriated U.S. Government funds through fraud. Incidents involving the property or appropriated funds of Army Reserve and Army ROTC will be investigated in the same manner as those involving the active Army with the thresholds established in AR 195-2. The degree of CID involvement will be determined by the CID supervisor. In reaching this decision, consideration will be given to such factors as the total amount of loss to the U.S. Government, seriousness of the offense, whether or not the offense is being investigated effectively by civil police or other federal law enforcement agencies, impact on CID investigative resources and the benefits to accrue to the U.S. Government as a result of a CID investigation. Responsibility for any collateral reporting will be determined in coordination with the provost marshal concerned.

2-7
Investigations involving Army National Guard

a. Federalized National Guard personnel are subject to the provisions of the UCMJ. Crimes perpetrated by Army National Guard personnel not on active duty under Title 10 USC, will normally not be investigated by the USACIDC except as noted below. The USACIDC will investigate crimes within its purview committed by non-federalized Army National Guard personnel while on military reservations in the same manner as for other civilians. The USACIDC is authorized by AR 10-87 and AR 195-2 to initiate criminal investigations into offenses involving federal property or funds entrusted to the Army National Guard. USACIDC units should investigate allegations of significant criminal activity targeted against these federal assets. Within the limits of existing resources, proactive efforts, including crime prevention surveys, should also be undertaken to identify or prevent fraud, waste or abuse involving these same assets.

b. A USACIDC unit will also respond to a request for investigation received from the following individuals:

(1) Chief, National Guard Bureau or his designated representatives. These requests will be referred through the Commander, USACIDC, ATTN: CIOP-COP-PO.

(2) The State Adjutant General or the State U.S. Property and Fiscal Officer (USPFO). Requests for investigations from these individuals should be referred to the appropriate` USACIDC major subordinate command.

c. In determining whether to initiate an investigation, the following factors should be considered:

(1) The matter to be investigated must involve U.S. Government property, funds, or contracts (this would not preclude CID involvement if both state and federal property or funds were involved in the incident).

(2) Normal coordination with the FBI and appropriate U.S. attorney will be accomplished as prescribed in the 1984 Department of Defense/Department of Justice Memorandum of Understanding (MOU).

(3) The threshold levels for CID investigation as specified in AR 195-2 have been met.

(4) The benefits to accrue to the Federal Government as a result of the investigation must justify the personnel and monetary resources to be expended. For example, it may not be cost effective to send an investigator to a remote location to investigate the larceny of a single piece of equipment just meeting the threshold value with no obvious investigative leads to identify a perpetrator.

d. Investigation of offenses occurring on Army installations under the exclusive jurisdiction of the U.S. Government and involving National Guard personnel or property (either federal or state) will be investigated by the USACIDC in accordance with AR 195-2 and this regulation.

e. Investigations will be conducted in accordance with the policies and procedures normally followed by USACIDC elements in the conduct of their investigations. Maximum coordination should be accomplished with local civil authorities. Once initiated, an investigation may only be terminated by the USACIDC in accordance with the procedures prescribed in this regulation.

f. All CID units may, within the limits of available resources and the restraints of the Posse Comitatus Act, assist state agencies in investigating leads involving the active Army or which require expertise peculiar to CID.

g. Incidents involving offenses against National Guard property for which the USPFO is not responsible (e.g., administrative sedans, buildings, typewriters, etc.) will not normally be investigated by the USACIDC.

h. Each USACIDC element that conducts an investigation involving a state National Guard unit or member will personally brief and coordinate all investigative activity as is normally required. All CID reports will be distributed personally to the state adjutant general; however, this must be accomplished in the most cost effective manner. When a CID report is prepared for distribution to the state adjutant general, preliminary telephonic coordination will be made. This coordination will address the fact that a CID report is being forwarded, normally by U.S. postal channels, to the state adjutant general's office. Field elements will use two envelopes to forward these reports. An outer envelope will bear the address of the state adjutant general's office while a second inside envelope will be personally addressed to the state adjutant general and marked "eyes only for addressee". The USACIDC field element forwarding this report will subsequently contact that individual to ensure receipt of the report. The mode of delivery must ensure the most direct, personal, and expeditious delivery. If appropriate, copies will also be provided to the U.S. attorney or state attorney general responsible for prosecuting any criminal offenses. Information copies will be provided to the Chief, NGB, ATTN: NGB-IG. Reports of action taken, as required by AR 195-2, will be provided by the state adjutant general.

2-8
Violations by U.S. Army Recruiting Command (USAREC) personnel

Special procedures have been developed by MOU with USAREC for investigation of recruiting violations by USAREC personnel. Refer to paragraph 4-29 for procedures concerning recruiting violations.

2-9
Investigations involving the U.S. Army Corps of Engineers (USACE)

a. The USACIDC units have authority to and responsibility for investigating criminal acts affecting activities of the USACE or committed by its employees in the conduct of their official duties as governed by the provisions of DoD Instruction 5505.2. This includes crimes committed at or affecting civil works projects or sites. However, because of the wide area over which these activities and job sites are located, often at considerable distances from any Army installation, this authority to investigate must be exercised with sound judgment. In determining whether to undertake the investigation of a property-related offense, consideration must be given to such factors as the seriousness of the offense, total amount of actual or potential loss to the U.S. Government, whether the offense is being investigated effectively by civil police, impact on CID resources, and benefits to accrue to the government as a result of a CID investigation. Responsibility for any collateral reporting will be determined in coordination with the proper provost marshal.

b. Loss of appropriated U.S. Government funds through fraud that involves any USACE unit or personnel will be investigated in accordance with the thresholds established in AR 195-2.

CHAPTER 3

Section I Authority

3-1
Authority

All USACIDC special agents (military or civilian) are recognized as federal agents (law enforcement officers) under 28 Code of Federal Regulation (CFR), section 60.3 (a) (2).

3-2
Authority to administer oaths

Special agents (military or civilian) have the authority to administer oaths pursuant to 10 USC 936 (Article 136, UCMJ) or 5 USC 303, respectively, when conducting investigations.

3-3
Civilian special agents

a. Normally USACIDC's civilian special agents are assigned to the mission of investigating major procurement acquisition contract frauds. Although their primary mission is that of acquisition contract frauds, they may be utilized in other are as, when circumstances or Army interests require a USACIDC response, or as determined by the Commander Investigative Services Activity (ISA), USACIDC or the Commander, USACIDC.

b. Civilian special agents assigned to procurement fraud units operate according to specific procedures outlined in chapter 11 and other appropriate guidance in this regulation.

3-4
Authority to apprehend/detain

a. Refer to 10 USC 807 (Article 7, UCMJ), Rules for Courts Martial (RCM) 302, and AR 195-2, for USACIDC authority to apprehend and/or detain.

b. Special procedures apply under RCM 302 for apprehensions which are to take place in a "private dwelling". An apprehension authorization may be required for such apprehensions. See chapter 5 of this regulation for guidance in this area.

c. Special agents have no statutory arrest authority over civilians outside a military reservation but may arrest civilians under citizen's arrest authority, if local

law so provides, when the situation leading to the arrest occurred by chance and not as an intended consequence of the special agent's official duties. When making arrests under this provision, special agents will not present themselves as acting in their official capacity as special agents. Civilians arrested outside a military reservation will be immediately released to the appropriate civilian law enforcement agency.

d. Unless required by exigent or life threatening circumstances, public or mass apprehensions in the presence of a command formation are not authorized. Such activities raise issues of unlawful command influence affecting due process. Furthermore, this type of public apprehension results in needless intimidation, embarrassment and ridicule, actions that are contrary to the professional image of Army CID agents.

3-5
Authority to search and seize/serve warrants of attachment

a. Refer to Military Rules of Evidence (MRE) 312, 314-317, Manual for Courts-Martial (MCM)(2000), AR 190-22 with USACIDC supplement, AR 195-2 and AR 27-10 for detailed procedures on search and seizure within the military. See chapter 5 of this regulation.

b. Within the United States and its territories, special agents may seek and execute federal search warrants pursuant to Rule 41 of the Federal Rules of Criminal Procedure when there is probable cause to believe that the search will result in the seizure of evidence of a crime that is within the investigative jurisdiction of the Army. The USACIDC special agent is included in 28 Code of Federal Regulations (CFR) Part 60 amongst the federal law enforcement officers authorized to seek and execute federal warrants (18 USC 3105). A CID agent may also be called upon to serve warrants of attachments (DD form 454) on civilian witnesses in courts-martial in the United States, its territories and possessions, to compel by R.C.M. 703 (e)(2)(G) the presence of a witness or the production of documents at the court-martial. Under these provisions, USACIDC special agents must first coordinate with the local supporting SJA office and obtain the concurrence of the appropriate U.S. attorney before seeking the warrant or serving a warrant of attachment on civilians off of the installation.

c. Federal Rules of Criminal Procedure, Rule 41, requires that search warrants "shall be directed to a civil officer of the United States authorized to enforce or assist in enforcing any law thereof or to a person so authorized by the President of the United States." Pursuant to 28 CFR Part 60 and Executive Order 12473, MCM, United States, 1998, Rules for Courts-Martial 302(b) and Military Rules of Evidence 315(h), civilian and military criminal investigators assigned to the USACIDC are given authority sufficient to bring them within the category of persons authorized by the President to enforce or assist in enforcing the laws of

the United States. Accordingly, civilian and military investigators assigned to the USACIDC meet the requirements of Rule 41(c), Federal Rules of Criminal Procedure, and are authorized to serve and execute search warrants issued pursuant to Rule 41.

d. Criminal investigators serving or executing search warrants off military installations pursuant to this authorization shall ensure that they are accompanied and assisted by a law enforcement officer having statutory authority to make an arrest in the event that such action becomes necessary.

e. USACIDC special agents are authorized and encouraged to make use of administrative subpoenas. Although intended primarily for use in economic crime investigations, a subpoena may be obtained, when appropriate, for use in any USACIDC investigation. See chapter 5 of this regulation.

f. Outside the United States, the authority of special agents to conduct searches and seizures outside the military installation will be governed by status-of-forces or similar agreements, and locally established search and seizure policies.

3-6
Authority to use and bear arms

a. See AR 190-14, AR 195-2 and chapter 17 of this regulation for information concerning authority and policy on the carrying of weapons and use of force.

b. Prior to any official travel (except as noted in c below) during which a weapon will be carried into or through a country other than in which permanently stationed, the special agent(s) will determine the legality of and procedures for bringing a weapon into the countries involved. This includes temporary stops; i.e., change of aircraft, refueling, etc. The appropriate USACIDC major subordinate command will coordinate with the Regional Security Officer (RSO), U.S. Embassy, in each country involved in the travel to obtain this information.

c. Requests for weapons and country clearance pertaining to a protective services mission will be made through the Protective Services Unit, USACIDC. Prior to travel, USACIDC major subordinate commands will provide the following information via message to CDR PSU FT BELVOIR VA //CISAP-ZA// pertaining to special agents who will support protective service missions: NAME, SSAN, DOB, POB, passport number, date and place of issue of passport, and the caliber, make, model, and serial number of the weapon to be brought into the country where the mission is located. When possible, arrival information should also be provided.

3-7
Pursuit Driving

a. Pursuit driving occurs (commonly referred to as “hot pursuit” by most law enforcement agencies) when the pursuit exceeds or violates existing traffic laws. While not prohibited, pursuit driving by special agents is discouraged and should only be undertaken in situations where the fleeing felon's threat to public safety/national security clearly outweighs the accompanying dangers to the agent(s) and the public. Pursuit driving is an inherently dangerous activity, particularly for non-uniformed police officers in unmarked vehicles. Hot pursuits should not be conducted by special agents without vehicles properly equipped with operable emergency lights, siren, communications ability with local law enforcement and Military Police (MP), along with pursuit or emergency driver’s training for the agent driver.

b. Special agents may pursue violent felony violators (e.g. murder, rape, armed robbery), but will not engage in pursuits pertaining to misdemeanor or non-violent felony violators. If the special agent determines there is a need for a high-speed pursuit, the following will be strictly adhered to:

(1) The MP and local law enforcement as appropriate will be notified of the pursuit, description of the vehicle, location and direction of the pursuit, and offense facilitating the pursuit. Special agents should request for MP or law enforcement back-up. The CID supervisor should be notified of the pursuit and its results as soon as possible.

(2) Pursuits will only proceed off the installation if allowed by local policy coordinated per paragraph 3-7c below. If pursuit proceeds off the installation, the agent will ensure the MP desk notifies local police of the pursuit, and request their assistance. The MP desk should be periodically updated on the status of the pursuit. Upon the local police engaging in the pursuit, the special agent will turn over the lead vehicle position to the local authorities, and follow at a safe distance and speed.

(3) Safety will not be sacrificed at any time. If a special agent engages in a pursuit, he/she should continually evaluate the situation, and terminate the pursuit when the risk to the public and/or the special agent outweighs the need to immediately apprehend the suspect. If at any time the special agent loses sight of the violator, the pursuit will be terminated. Upon termination of a pursuit, other resources (i.e., military and/or local law enforcement, radio alerts, be-on-the-lookout bulletins, NCIC identification, license plate checks, etc) should be considered to identify suspects and facilitate their later apprehension or arrest

(4) If the violator is halted in civilian jurisdiction, a felony traffic stop will be conducted. The violator will be detained until the arrival of the civilian law

enforcement authorities. If the civilian authorities agree, the violator will be transported to the installation under military law enforcement control, if not, the violator will be relinquished to the civilian authorities.

c. The CID investigative element commander or SAC will issue written policies pertaining to pursuits, taking into consideration the information contained in this paragraph along with any local, state and host nation restrictions pertaining to this issue. The hot pursuit policy should be coordinated with local, state, host nation law enforcement and legal authorities, as well as the Provost Marshal (PM). The local CID pursuit policy should be consistent with that of the local Military Police. Local CID pursuit policy will conform to local, state, and host nation laws and policies.

d. If a hot pursuit results in physical injury or damage to property, the information will be reported to a CID supervisor immediately or as soon as possible. The information will be reported to HQUSACIDC CIOP-ZA within four hours of the incident. The information will also be reported to the local PM and installation commanders.

3-8
Prior approval required

Special agents will not be assigned to full-time covert investigative duties without the prior written approval of the USACIDC major subordinate commander. Written approval will indicate the date, time, and place that the special agent(s) are to begin working in a covert status, the specific activities of the special agent(s) involved in the operation, and the estimated date the agent(s) will be returned to normal investigative duties. This does not limit the authority of CID supervisors to utilize assigned special agents for routine investigations where they are working in a semi-covert capacity (e.g., drug teams, etc.).

3-9
Assumed military role

a. The special agent-in-charge (SAC), operations officer, or commander may authorize assigned special agents and attached persons to assume a short-term military role and display the insignia of a person of lower or higher pay grade than that actually held by the individual during the conduct of a specific investigation. Short term is defined as a period during which the special agent will be able to function in the military role without actually performing duty with another unit or being assigned to another unit (e.g. purports to be TDY or on leave in the area for periods consistent with TDY or leave status).

b. USACIDC major subordinate commanders may authorize assigned special agents and attached personnel to assume a full-time military role and display the insignia of a person of lower pay grade than that actually held by the individual during the conduct of a specific investigation. However, the role will not include that of a person providing medical, legal, or chaplain services. Full-time military role is defined as a role requiring official assignment to another unit, assumption of duties with that unit, and full administrative support by that unit.

c. In instances where there is a need for a special agent or attached person to assume a full-time military role and display the insignia of a person of higher pay grade than that actually held by the individual, or to assume the role of a chaplain, attorney, or a person providing medical services, a request outlining the requirement will be forwarded through channels to the Commander, USACIDC, ATTN: CIOP-ZA, for appropriate action and approval.

3-10
Obtaining identification cards and ration control documents for covert special agents

a. When necessary, each USACIDC major subordinate commander will establish standard operating procedures (SOP) pertaining to the acquisition, use, and control of identification cards and ration control documents for use in covert operations. A control log may suffice for the use of identification cards if it is determined that a SOP is not needed.

b. The SOP will, as a minimum, require a log to be maintained to reflect the number of each card obtained, the date of issue, the person receiving the card, the name and SSAN in which the card is issued, the date of return of the card, and the date of destruction of the card. When the card(s) are no longer required for covert operations, they will be destroyed and the destruction certified.

3-11
Obtaining operational nicknames

a. All operational nicknames are coordinated with the Army Operations Center (AOC), Headquarters, Department of the Army (HQDA). Each operational nickname consists of two words. The FIRST word is issued by HQDA, with the SECOND word determined by the requesting organization. Requests for operational nicknames by individual USACIDC investigative elements will be approved by the USACIDC major subordinate command. Upon approval, the request will be made by the USACIDC major subordinate command and directed to HQUSACIDC, ATTN: CIOP-COP for coordination and appropriate action. The request will be in memorandum format and contain the following information:

(1) The identity of the requesting USACIDC investigative element.

(2) The type of operation (covert, semi-covert, taskforce or joint) and the focus of the investigation (drug suppression, fraud crimes, or other types of economic, persons or property crimes) being targeted.

(3) Where (location/area) the operation will occur.

(4) When the operation will begin (date).

(5) When the operation will end (date).

(6) The SECOND WORD of the operational nickname.

b. HQUSACIDC will coordinate the request with HQDA and obtain the FIRST WORD of the operational nickname. Once approval of a complete nickname is obtained, the requesting major subordinate command will be notified. The operational nickname is valid only for the specified period of time. In the event the operation extends beyond the initial time period, the requesting major subordinate command must notify HQUSACIDC, ATTN: CIOP-COP for an extension.

c. Commanders of major subordinate commands should carefully consider each operational nickname request, as not all covert operations have a need for a nickname.

3-12
Civilian clothing and non-standard appearance

a. As authorized by AR 195-2 and AR 670-1, special agents will wear civilian clothing in the performance of their normal investigative duties.

b. Civilian clothing worn by special agents will be in good taste and commensurate with clothing worn by the business or law enforcement sector of the community in the area in which they are operating or as dictated by the specific investigative duties which they are assigned.

c. All CID supervisors are responsible for ensuring that clothing worn by special agents is appropriate for the duties to be performed and suited to the prevailing climatic conditions.

d. Special agents and other investigative personnel under USACIDC operational control, will adhere to the personal appearance and grooming standards of AR 670-1 unless performing specific investigative duties for which non-standard appearance has been authorized by the USACIDC major

subordinate commander. Requests for exception to those standards will be forwarded through the chain of command and will not normally exceed periods of 90 days. Authority for approval of non-standard appearance may be delegated to the district or field office commander, in which case a copy of the authorization for exception will be furnished to the USACIDC major subordinate commander.

3-13
Military clothing

a. The provisions of the preceding paragraph do not preclude the wearing of the military uniform when its wear would be appropriate.

b. Special agents attending military schools will wear the appropriate uniform with their respective rank and unit insignia, where the military uniform is the proper attire.

c. In accordance with AR 670-1 and AR 195-2, special agents are authorized to wear the subdued "U.S." insignia in lieu of insignia of rank when wearing field uniforms and participating in combat training or operations. Staff personnel assigned to CID headquarters elements will normally wear their respective insignia of rank. All other special agents involved in such activity in field uniform will wear the subdued "U.S." insignia. Manner of wear of the subdued "U.S." insignia is as follow s:

(1) Utility shirts. Centered horizontally on left and right collars, 1 inch from the lower edge of the collars.

(2) Cold weather coats. Centered on the shoulder loops, 5/8 inch from the outside shoulder seam, with the bottom edge of the insignia facing the shoulder seam.

(3) Black beret and, when applicable, battle dress uniform (BDU) caps. Centered on the flash or cap, respectively, left to right, top to bottom.

(4) Helmet camouflage covers. Centered on the front of the cover, approximately 2-1/2 inches up from the bottom rim.

d. All CID special agents wearing the field uniform when performing investigative duties will wear the CID brassard, unless its wear would be detrimental to mission accomplishment. See AR 670-1.

3-14
Disclosure of grade.

AR 195-2 contains information concerning the Army's policy on disclosure of grade of USACIDC agents.

3-15
Billets and messes

See AR 195-2 for information concerning the billeting and messing of enlisted special agents and USACIL examiners.

3-16
Freedom of movement

a. Special agents are authorized freedom of movement within the geographical area of responsibility of the USACIDC unit to which they are assigned.

b. Special agents may enter the area of another USACIDC unit to complete an investigation rather than forwarding a request for assistance. In these instances, prior coordination will be effected between USACIDC units.

c. When specifically authorized by the CG, USACIDC, special agents may enter any area without notification to, or briefing of, the CID commanders involved.

d. All USACIDC personnel must obtain Special Area, Country and/or Theater clearance for any travel outside the United States, its territories and possessions. In some cases, all, one or more, or none of these clearances may be required. The individual country pages listed in the DOD Guide 4500.54-G, DOD Foreign Clearance Guide (FCG) General Information Booklet (www.fcg.pentagon.mil/fcg/fcg.htm) should be consulted when planning to travel. The lead time for requesting travel clearances varies with each individual country, so the FCG should be checked. Travel will not be undertaken without having the appropriate approved travel clearances.

(1) Travel clearances may not apply to personnel in Unified or overseas commands traveling to subordinate units of those commands, to intra-theater troop movements, and to personnel deploying to support formally approved exercises or contingency operations. However, coordination with appropriate travel managers should still be effected to ensure travel clearances do not apply before proceeding on any travel to a foreign country.

(2) Airlines, transportation authorities, etc. need only ensure that travelers have the proper identification credentials and entry requirements (passport, visa,

ID card, orders, etc.) to process through border clearance facilities. Ensuring the traveler has the appropriate travel clearance (Special Area, Country and/or Theater) is the responsibility of the traveler, his/her unit, and the clearance granting authority.

(3) In some special circumstances related to the type of planned contacts, meetings, and/or security classifications (as specified in AR 55-46, Travel Overseas), additional clearances may have to be requested through the Office of the Secretary of Defense to the Department of State.

(4) In all cases of foreign travel, USACIDC personnel will obtain pre-travel security briefings per AR 381-12 from the appropriate security manager. Further, USACIDC personnel will also obtain pre-travel terrorist and force protection briefings from the appropriate force protection officer per AR 525-13.

(5) Types of Personnel Travel Clearances and Documents:

(a) Special Area: The Department of State and the Office of Secretary of Defense designate certain countries as "Special Areas." Clearance is required from the Department of State through the Office of the Secretary of Defense to travel to these countries. Request Special Area clearance concurrently with Country and/or Theater clearance. Check the individual country pages of the FCG for information.

(b) Country Clearance: A clearance required from the American Embassy (through the U.S. Defense Attaché, the Office of Military/Defense Cooperation, the Military Advisory and Assistance Group, etc.) for travel to that country. Approval applies only for visits to that country for a stated purpose. Country clearances may be required, assumed, or not required if visits are only to US military facilities in that country. Consult individual country pages in the FCG for information.

(c) Theater Clearance: A clearance required for visits to overseas military activities on matters pertaining to the mission of the Unified Command. Clearance is granted by the Unified Command or may be delegated to subordinate commands, special agencies or units to be visited. Clearances may be required or assumed. Consult the individual country pages of the FCG for information.

(d) International Agreements: Approval of certain foreign governments for US personnel to enter their territory for defense purposes is included in Status of Forces Agreements (SOFA) or Military Rights Agreements. However, some agreements (e.g., NATO SOFA) require US personnel to have a specific type of identification document (ID card, orders, etc). These requirements are reflected on the individual country pages of the FCG.

(e) Passports: A passport does not constitute authority to enter any country. However, many countries have adopted procedures which permit US citizens to enter their territory without further documentation upon presentation of a US passport. Consult the individual country pages of the FCG for information.

(f) Visas: A visa is official evidence that a person has approval of a foreign government to enter its territory. Many countries require US personnel entering for defense purposes to obtain a visa. Individual country pages of the FCG reflect these requirements.

3-17
Safeguarding weapons and equipment during travel

a. See chapter 17 for provisions governing the safeguarding of weapons during travel.

b. Other sensitive or high-cost equipment (e.g., computers, cameras) will be protected in the following manner:

(1) By carrying on the person or otherwise keeping within the view of the special agent.

(2) By storing in normal baggage racks or compartments using luggage which does not identify the contents.

(3) By locking in the trunk of a vehicle.

(4) By placing in a locked room of a public lodging or by depositing with the keeper of the lodging.

(5) By affording a level of protection equivalent to the foregoing.

c. Polygraph instruments will not be stored in normal luggage racks or checked through as normal baggage. Due to the sensitivity of polygraph instruments, they will be hand carried during transit.

3-18
Standards of conduct

See DoD Directive 5500.7, Standards of Conduct; DoDD 5500.7-R, Joint Ethics Regulation (JER); Standards of Ethical Conduct for Employees of the Executive Branch, Part I of Executive Order 12674; AR 195-3, and 5 CFR, Part 26 35 for information on the standards of conduct applicable to CID supervisors, special agents, and other USACIDC personnel.

CHAPTER 4

4-1
Purpose

A criminal investigation is specific in intent and limited in purpose. It is always related to a known or suspected violation of a criminal law. It is not normally directed toward non-criminal activity such as administrative error, managerial deficiency, or negligence. The USACIDC investigations may need to-support other proceedings against subject(s) such as civil, administrative, and contractual. The objectives of a criminal investigation are:

a. Establishing whether or not any criminal offenses have occurred and, if so, what offenses.

b. Determining the identity of the offenders.

c. Discovering, evaluating, maintaining, and providing in a timely manner to appropriate authority all of the pertinent facts, to include the collection and preservation of potential evidence in a form which will render it admissible in a court proceeding.

4-2
Scope

a. When a USACIDC criminal investigation is initiated, the investigation will normally extend to all aspects of the case including related offenses, lesser included offenses, attempts, conspiracies to commit the primary or lesser included offenses, and accessories after the fact.

b. Not every possible aspect of the case need be investigated or listed in the report, but the guiding principle is that an investigation is not to be fragmented among multiple agencies without an overriding reason. Thus, if a complaint within USACIDC investigative purview is received that soldier A has committed an offense against Y and a simple assault against Z as part of one incident, the USACIDC will investigate and report both offenses. Similarly, if soldier B is apprehended while committing a robbery and, when searched, is found to be in possession of suspected marihuana, the USACIDC will investigate and report both offenses.

c. CID supervisors at all levels must closely monitor the initiation of case files and reports of investigation to ensure that attempts are not being made to increase workload productivity by "splitting" cases. A case is "split" when one incident encompassing multiple offenses or subjects is reported as several separate incidents listing the offenses or subjects separately. Manipulating such incidents and case numbers does nothing more than distort the overall picture

and give commanders and staff at all levels a false perception of the actual problem. There are times when "splitting" a case may be appropriate or even necessary to better manage and control the investigation, however, such instances should occur only on an exceptional basis. When such action is considered necessary, full justification will be presented in the Agent Activity Summary (AAS) and will be approved by the special agent-in-charge or operations officer.

4-3
Extent

Once initiated, a criminal investigation will be actively pursued until:

a. It is referred to another USACIDC unit.

b. It is referred to another investigative agency and that agency has requested the USACIDC to cease active investigation.

c. It is completed in that all logical and practical investigative leads have been exhausted.

d. It is terminated as authorized under paragraph 4-17.

4-4
Limitation of investigative effort

a. The USACIDC will often receive complaints of wrongdoing which include multiple allegations of criminal acts as well as administrative and contractual irregularities. In these situations, as soon as credible information is available, or as soon as the investigation has progressed sufficiently that a reasonable decision can be made, CID supervisors should coordinate with the appropriate legal advisors (local staff judge advocate, procurement fraud advisor, U.S. attorney, Defense Procurement Fraud Unit (DPFU)) to determine if any allegations have greater merit for prosecution or civil recovery by the government. If so, the investigation should then be focused on these particular allegations, with other issues being held in abeyance pending further development of the investigation which would indicate that those lesser issues should be pursued or that their investigation is not necessary to adequately protect government interests. It is recognized that, in some instances, these latter issues may be legitimate allegations of criminality which would normally require investigative action in a timely manner. Allegations which are not pursued will be documented in the final report of investigation, together with reasons for their not being investigated.

b. Where there are numerous criminal allegations from one or more individuals and the validity of the allegations cannot be otherwise readily determined, use of the polygraph should be considered early in the investigation prior to the expenditure of significant investigative effort and resources.

4-5
Receipt and development of complaints

a. Receipt of complaints

(1) When a USACIDC unit receives information that an alleged criminal incident has occurred which is, or may be, within USACIDC's investigative responsibility, a case file will be initiated and entered into the ACIRS database and a sequence number assigned in accordance with paragraph 6-2.

(2) When a USACIDC unit receives verbal notification of an alleged criminal incident, a verbal response is sufficient reply to indicate USACIDC's intent in the matter.

(3) When written notification of an alleged criminal incident is received, a written reply to the person or office reporting the incident may be furnished. The reply should state whether the USACIDC has accepted or declined investigative responsibility.

(4) When a criminal complaint is referred to the USACIDC by the military police, the appropriate provost marshal will be advised of the acceptance or declination of investigative responsibility by the USACIDC. When the initial notification is telephonic and the incident does not fall within the USACIDC investigative purview, a telephonic declination may be provided. When the conduct of a preliminary investigation reveals no requirement for a USACIDC investigation, the provost marshal will be provided with a memorandum summarizing the results of the preliminary investigation. When an ROI is initiated, the provost marshal will be provided a copy of the initial report and all subsequent reports. See paragraph 8-41 concerning authorized delays in distribution.

(5) When the HQUSACIDC receives referrals of criminal allegations from MACOM level elements and audit agencies such as the U.S. Army Audit Agency (USAAA) and Defense Contract Audit Agency (DCAA), the Deputy Chief of Staff for Operations (DCSOPS), USACIDC, will by a request for investigation (RFI), task the appropriate USACIDC major subordinate command to investigate the allegations. The receiving CID field element will comply with the RFI suspense date to evaluate and analyze the information and to conduct a preliminary inquiry. If information has been developed to reflect the allegations are credible and within the scope of USACIDC's investigative authority and responsibility, a

report of investigation (ROI) will be initiated and an initial report dispatched. If a ROI is not initiated, the results of the preliminary inquiry and reasons for no ROI will be provided to the Commander, USACIDC, ATTN: CIOP-COP.

(6) When a formal audit referral report is received from a DoD audit organization, a case file will be initiated and entered into the ACIRS database and the assigned sequence number will be immediately provided to the referring audit organization.

(a) If an ROI is initiated, the audit referral will be referenced in the investigative summary of the initial or initial/SSI ROI. A copy of the final ROI will be forwarded to the audit agency concerned by sending the report to the audit agency concerned through the Commander, USACIDC, ATTN: CIOP-COP.

(b) If an ROI is not initiated, a copy of the Summary of Action, Agent's Investigation Report (AIR) detailing why no ROI was initiated, and a copy of the audit referral, will be forwarded by memorandum of transmittal to Commander, USACIDC, ATTN: CIOP-COP, upon completion of the preliminary inquiry.

(c) If the receiving CID office does not have investigative responsibility for the allegations, the audit referral will be transmitted to the appropriate DoD criminal investigative organization for follow-up. The referring audit organization will be immediately furnished with the information on the investigative agency where the audit referral was transferred and the reasons for such action.

(d) When the audit referral allegation involves a U.S. Government contract, the receiving CID field element will coordinate with the audit organization to determine when and by whom the appropriate U.S. Government contracting office will be notified.

(e) The CID field element will establish contact with the audit agency upon receipt of the referral and will maintain close contact with the organization throughout the course of the investigation.

b. Development of complaints

(1) Investigative activity does not depend only upon the receipt of a complaint from an outside source. Complaints may be developed within USACIDC units from sources, target analysis files, crime prevention surveys, criminal intelligence reports, or as an outcome of another ROI.

(2) When an indication of an alleged criminal incident is developed by a USACIDC unit, the information may be recorded in an existing case folder providing it is closely connected with the case.

Monitorship of investigations

a. The DCSOPS, USACIDC, will monitor selected investigations to keep the CG, USACIDC, and higher level Army staff officials fully advised of the investigative developments and ensure the expeditious completion of the investigation. A USACIDC major subordinate commander may recommend that an investigation be monitored and the monitorship category to be designated. The DCSOPS, will notify the USACIDC major subordinate commander by message that command monitorship has been initiated.

b. To assist subordinate commanders in determining the level of priority to give each monitored investigation, the HQUSACIDC notification of the monitorship will specify one of the following categories to guide investigative efforts:

(1) Category I. Investigations monitored in this category have been identified by the CG, USACIDC, as a top priority investigation. It has precedence over all other investigative activities and requires immediate action by all USACIDC units. Any requests for assistance and laboratory requirements will be identified immediately and dispatched by the most expeditious means. Results will be provided to the office of origin within 24 hours of receipt. Reasons for non-compliance with the 24 hour response time limit will be expeditiously provided to the office of origin. The HQUSACIDC case monitor will be identified in the monitorship notification message. The case status will be provided to the case monitor by CID electronic mail, fax or electrical message to arrive NLT 1200 (EST) each Wednesday until the investigation is completed or the monitorship is terminated. Copies of all agent activity summaries, written statements, certificates, agent's investigation reports, photographs, narratives, and a copy of the final ROI will be provided to the case monitor as needed.

(2) Category II. Investigations monitored in this category have been identified by the Deputy Commander, USACIDC, as requiring precedence over all investigative activity other than category I monitorship investigations. Requests for assistance and laboratory requests will be dispatched by the most expeditious means. The results will be provided to the office of origin within three working days of receipt. Reasons for non-compliance with the three day response time will be provide d to the office of origin. The case status will be provided to the case monitor NLT 1200 (EST) each Wednesday, encompassing investigative activity accomplished as of 24 hours prior to the message. The monitorship notification and subsequent communications will contain instructions for providing investigative documents to the case monitor.

(3) Category III. These are special interest investigations. This type of case is essentially routine but has HQUSACIDC interest and is to be handled in an expeditious manner. This monitorship will normally be identified by the DCSOPS, USACIDC, based on requirements for special information papers and to keep the DA and the DoD staffs informed of developments in the investigation. Leads and

laboratory requests, when appropriate, will be identified as requiring priority processing. Any special handling will be identified by the HQUSACIDC case monitor on a case-by-case basis. The case status must be forwarded to the DCSOPS, case monitor, monthly. The case monitor will notify the major subordinate command of the date the case status is required. Monitorship of these cases may be terminated at any time by the DCSOPS based on an evaluation of the continuing requirements or on recommendation of the USACIDC major subordinate commander.

c. All evidence dispatched for USACIL examination will be clearly identified as pertaining to a monitored case and the monitorship category will be provided in the USACIDC request. The USACIL will give these examinations priority in consonance with the category of monitorship.

d. Requests for assistance to other USACIDC units will specify that the investigation is a monitorship case, identify the category, and provide the necessary suspense date.

e. Monitorship case updates will be submitted in the format shown at figure 4-1.

4-7
Purpose and procedures of preliminary investigations

a. The purpose of a preliminary investigation is to determine if there is credible information that a crime has occurred and if the USACIDC has investigative responsibility. If, at the onset, credible information exists and the USACIDC has investigative responsibility, a preliminary investigation is not required and a ROI will be initiated. Preliminary investigations will be conducted expeditiously and will not be used as a means of holding in abeyance a USACIDC decision to initiate a ROI. Field element supervisors will allocate the necessary resources to ensure preliminary investigations are conducted in accordance with established USACIDC investigative standards.

b. Supervisory review of preliminary investigations at higher headquarters (field office, battalion, group, and HQUSACIDC) may direct the initiation of a ROI if, in consideration of all relevant facts and circumstances, a ROI would better serve the interests of the USACIDC.

4-8
Results of preliminary investigations

Every preliminary investigation must result in one of the following actions:

a. A determination that there is no credible information that a crime occurred. In this case, the sequence number/ACIRS action will be completed and the investigative effort documented on the AAS.

b. A determination that there is some credible information that a crime occurred but the USACIDC lacks the authority to investigate. In this case, the appropriate investigative agency will be notified and the sequence number/ACIRS action completed. A summary AIR will be prepared explaining the investigative effort.

c. A determination that there is some credible information that a crime occurred, and the USACIDC has the authority to investigate but does not have investigative responsibility. In this case, the appropriate investigative agency will be notified, the sequence number/ACIRS action completed, and an AIR prepared, unless a determination is made to assume investigative responsibility pursuant to AR 195-2, in which case, a criminal investigation or collateral report, as appropriate, will be initiated.

d. A determination that there is some credible information that a crime occurred and the USACIDC has investigative responsibility. In this case an ROI number will be assigned and the case will be investigated by USACIDC.

e. When the USACIDC does not have investigative responsibility, special agents should take immediate action to preserve crime scenes and related evidence pending the arrival of appropriate investigative authorities.

f. Preliminary investigation of any alleged child abuse, which does not result in a ROI, will be completed on a sequence number action. The USACIDC disposition of the incident, reasons for disposition, and any coordination accomplished in conjunction with the inquiry will be recorded in an AIR and in ACIRS. The suspect’s information will be indexed in ACIRS under the “Subject Name” field and the victim’s information will be entered in the “Victim Name” field. The synopsized results of the preliminary investigation will also be annotated in the “Memo” field of the ACIRS database.

g. Preliminary investigations which do not result in a ROI will be completed on the sequence number/ACIRS action. USACIDC disposition of the incident, reasons for disposition, and any coordination accomplished in conjunction with the inquiry will be recorded either in the AAS or AIR.

h. The contents of a sequence number action file will be released with the approval of the special agent-in-charge or operations officer. A memorandum of transmittal (see figure 4-2) may be used to forward the contents.

i. Additionally, a memorandum of transmittal should be used to forward the contents of a sequence number action file to other USACIDC units.

Procedures for Criminal Investigations

a. Criminal investigations will be initiated as follows:

(1) A USACIDC report of investigation (ROI) will be initiated when there is credible information that a crime has or may have occurred and the USACIDC has investigative responsibility. A ROI number will be assigned as soon information is obtained that would cause a trained investigator under similar circumstances to pursue further the facts of the case to determine whether a criminal act occurred or may have occurred. Any investigative activity (i.e., interviews, scene examination, searches, surveillance, source targeting, etc.) beyond mere evaluation of the complaint or allegation requires the initiation of a ROI. The fact that a referral to a non-USACIDC agency is anticipated, that there exists a possibility that the offense(s) will eventually be unfounded, or that the complainant has provided a false or inaccurate report, does not negate the requirement to assign a ROI number. A USACIDC criminal investigation will be initiated for crimes listed in Appendix B of AR 195-2 and other crimes deemed appropriate in accordance with AR 195-2 or other applicable criminal statute(s). The only exceptions to the ROI requirement are semi-covert drug suppression targeting and the four step approach used in the conduct of Target Analysis Files (TAF) IAW paragraph 10-20 of this regulation.

(2) In instances where a complainant alleges that a criminal offense having an Army interest occurred at a location outside the area of responsibility (AOR) of the USACIDC field element receiving the complaint, and no related criminal offenses have occurred in the AOR of the field element receiving the complaint, the following procedures apply:

(a) A sequence action will be initiated in accordance with paragraph 4-5a(1). The complaint and all other known or developed information will be immediately forwarded to the field element responsible for the area in which the crime occurred by a memorandum of transmittal. Prior telephonic or electronic mail notification will be made by the transferring field element to the field element to whom investigative responsibility is being transferred. The telephonic or electronic mail notification will be made by the close of business of the next business day following receipt of the complaint. If credible information is present that a crime has occurred, the field element having responsibility to investigate will initiate an ROI based on the notification of the pending transfer. The field element having responsibility to investigate will ensure that timely reporting of the appropriate Initial, Initial/SSI and SSI Only ROI is accomplished in accordance with standards established in this regulation. If credible information is not present, the field element having responsibility to investigate will initiate a preliminary inquiry to suspense the receipt of documents and to initiate investigative procedures based on the priority/urgency of the matter being reported. The following actions will be taken by the field element receiving the initial complaint:

1. A detailed written statement will be obtained from the complainant/victim in accordance with statement taking procedures addressed in this regulation.

2. Other individuals pertinent to the allegation and present within the AOR of the field element receiving the complaint will be interviewed and processed as required based on their involvement in the incident.

3. Available physical evidence will be collected.

4. The written statement of the complainant/victim, other statements, police reports, activity summaries, interview work sheets and all other pertinent documents will be forwarded to the field element responsible for the area in which the crime occurred. Information in the ACIRS database will be transmitted electronically. Hard copy transmittal of that data is not required. The documentation will be forwarded by a memorandum of transmittal within five working days of receipt of the complaint. A DA Form 209 or equivalent notice will be forwarded with the memorandum of transmittal. The receiving field element will annotate the DA Form 209 and return the form to the originating field element. This form will be placed in the file pertaining to this action. An alternate method for the DA Form 209 is for the originating field element to request electronic mail acknowledgment in the memorandum of transmittal.

5. Physical evidence collected will not be forwarded until the receiving field element provides the address of the evidence room that supports the receiving field element. This information may be included on the DA Form 209, provided telephonically or by other means deemed appropriate.

6. The originating field element will not close their file until the DA Form 209 or electronic mail acknowledgment has been received and the evidence dispatched to the receiving field element.

7. The field element responsible for the area in which the offense occurred will process the documentation from the originating field element in accordance with the provisions of this regulation and AR 195-2.

8. If there are other factors that would warrant the field element receiving the original complaint to conduct the investigation, e.g., the majority of the victims, suspects, and witnesses are in the AOR of the field element receiving the complaint; the complaint will be handled in accordance with this regulation. The mere fact that the crime occurred in another area does not, by itself, constitute sufficient grounds to forward a complaint. Situations which involve more than one USACIDC major subordinate command, wherein there is a question or a dispute as to who should initiate and control the ROI, will be referred to the DCSOPS, HQUSACIDC, for determination.

(b) If the field element receiving the original complaint elects to initiate an ROI, the investigative responsibility will remain with that field element. However, transfer of investigative responsibility by a field element having initiated an ROI may be necessary under unique situations such as termination of a contingency mission or office closure. Because of the administrative burden control transfers pose, the object is to limit transfers to only mission essential situations. A transfer between field elements within the same USACIDC major subordinate command requires approval of that major subordinate commander. A transfer between two USACIDC major subordinate commands requires approval of both USACIDC major subordinate commanders before the transfer occurs. Disputes between major subordinate commanders about initiation and transfer of an ROI will be referred to the DCSOPS, HQUSACIDC for resolution. After transfer of investigative responsibility is approved, the transferring field element will close the ROI and forward the report, pertinent documents and evidence to the gaining field element. The gaining field element will initiate a new ROI and reference the previous ROI. Both ROI numbers, to include the primary offense code, will be placed on all documents with the transferring field element's ROI number in parentheses.

1. If the actual or alleged offenses involve conduct related to the official duties of a staff judge advocate (SJA), military judge, member of the Trial Defense Service, or civilian attorney (e.g., obstruction of justice on the part of a defense attorney), all available information will be reported expeditiously to the DCSOPS, USACIDC, prior to the initiation of an investigation or SSI only report. The DCSOPS, in coordination with the HQUSACIDC Staff Judge Advocate, will provide instructions as to the manner in which to proceed with the investigation.

2. If the actual or alleged offense involves conduct unrelated to official duties (e.g., assault on a child under the age of 16), the investigation will be initiated and a SSI submitted in the normal manner. However, the investigation will be controlled by the appropriate battalion operations officer or commander and conducted by a special agent(s) detailed from a USACIDC unit other than that which supports the organization to which the JAG officer is assigned.

b. Procedures involving U.S. treasury checks

(1) The USACIDC will not initiate an investigation as a result of a report of non-receipt or loss of a U.S. treasury check. Persons making such reports will be referred to the servicing finance and accounting office (FAO) to complete a stop pay order if they have not done so previously. The value of a check, regardless of whether or not it is negotiated, is the face amount of the check.

(2) If the original check has been cashed, the Division of Check Claims (DCC), U.S. Treasury, will send a copy of the check and a claim form to the person reporting the non-receipt.

(3) If the person completes and returns the claim form indicating that he/she did not cash the check, the DCC will task United States Secret Service (USSS) to investigate.

(4) If the claim form is not returned, the DCC will take no further action. Any casual payments made to the individual as a result of the report of non-receipt will be collected automatically.

(5) If the original check has not been negotiated at the time of the receipt of the stop-pay order at the DCC, the DCC will take no action unless the original check is subsequently cashed.

(6) If the original check is subsequently cashed, the original check, the claim form, and a request for investigation will be provided to the appropriate USSS office by the DCC.

(7) Any USACIDC field element may become involved in these investigations upon referral, or declination, of investigative interest from their servicing USSS office.

(8) In the event some other crime (e.g., robbery) normally investigated by the USACIDC is involved, the USACIDC will investigate immediately; however, no request for checks will be forwarded to the servicing USSS office until after it is known that the check has been cashed. The victim will be referred to the FAO for submission of a stop-pay order. The negotiation of the check will become known as a result of the USSS receiving a request for investigation from the DCC.

(9) A ROI will not be kept open solely pending receipt of a check from the DCC via the USSS unless it is known that the check has been negotiated.

(10) When a USSS office conducting an investigation, as a result of a DCC tasking, requests assistance from the USACIDC, the assistance will be provided in accordance with existing procedures for handling requests for assistance from outside agencies.

(11) If a complainant is in possession of a copy of the reported stolen check and forgery is alleged, the appropriate OCONUS USACIDC unit will initiate a ROI and conduct an investigation. When all investigative leads have been exhausted except for the receipt of the original negotiated check, the ROI may be closed as a Final (C). Upon receipt of the original check, a 1st Supplemental Report will be initiated. Additional investigative leads will be pursued, as deemed appropriate, by the CID supervisor.

c. Procedures involving insufficient/non-sufficient fund personal checks.

(1) The USACIDC will only investigate incidents of insufficient/non-sufficient fund personal checks in an aggregate amount of $1,000 or more, drawn by the same person or entity, when intentional fraud has occurred. For the purposes of this regulation, intentional fraud is considered to exist if all collection procedures normally followed by the check cashing activity have proven unsuccessful, or if the check was drawn on an account that was nonexistent or closed at the time of the writing.

(2) It is the responsibility of all appropriated and nonappropriated fund activities, banking or financial facilities, and other check cashing activities located on installations or locations under control of the U.S. Army, to make use of established installation or activity collection procedures, regarding insufficient/non-sufficient fund personal checks. If deemed appropriate, other legally recognized options to effect payment of any amount due should be discussed prior to the initiation of a criminal investigation.

(3) If the insufficient/non-sufficient fund personal check was written to an AAFES activity, an AAFES contractor bank will attempt collection from the customer. If voluntary collection fails, the account will be sent to AAFES headquarters for collection from the individual’s pay or other available means.

(a) In those instances where the individual alleges his/her dishonored check was forged and cashed by someone else, the contractor bank will require a forgery affidavit to be filled out by the customer. The bank will instruct the customer to make a complaint report to the servicing law enforcement authority. The original checks, along with the forgery affidavit, and police report number, if available, will be forwarded to AAFES headquarters.

(b) These original checks will be retained at AAFES headquarters for 180 days and, if not requested as evidence, will be destroyed. All other dishonored checks (i.e., non-sufficient funds, closed account, stop payments, etc.) will be retained by the contractor bank for 180 days. After 180 days, the checks will be scan copied and the originals destroyed.

(4) On a case-by-case basis, USACIDC may investigate insufficient/non-sufficient fund personal check incidents which have not met the aforementioned criteria when deemed appropriate and after considering the totality of the circumstances.

(5) Inspector General, DoD, subpoenas will be issued in criminal investigations into issuance of "bad check" by service members and DoD employees (including employees of military departments) only where there is evidence of actual financial harm to the U.S. Government of at least $1,000. This policy will apply regardless of the rank or location of the individual(s) under investigation in connection with the issuance of bad checks.

(a) All requests for original checks as evidence in criminal investigations will be forwarded thru the Fort Hood RA to the CID Liaison at HQ, AAFES. At the time of the request, all possible social security numbers (SSANs) under which the checks were written, should also be provided, if known. This will give AAFES the opportunity to cover all the possibilities during the initial request and will preclude undue delays from subsequent follow-up requests."

d. Procedures for conducting investigations of counterfeit U.S. Government obligations, U.S. currency, and counterfeiting equipment.

(1) It is the responsibility of the United States Secret Service (USSS) to investigate incidents involving the counterfeiting of U.S. Government obligations and to prevent the illegal manufacture and use of U.S. currency and counterfeiting equipment.

(2) When the USACIDC is in receipt of information or recovers evidence concerning suspected counterfeit U.S. Government obligations, a CID investigation will be conducted and a report of investigation (ROI) initiated. The appropriate offense and DIMIS code(s) will be entered into the ACIRS as well as documenting any known serial numbers of suspected U.S. currency. The nearest USSS office will be notified. The resulting coordination should establish the initiation of a Joint or Referred ROI, with the USSS as the lead agency.

4-10
Referral of investigation

a. Referral of an investigation is the transfer of investigative responsibility from a USACIDC unit to a non-USACIDC agency. Investigations will be referred only when:

(1) All of the alleged offenses are outside of the normal investigative responsibility of the USACIDC and there are no overriding reasons for the USACIDC to assume investigative responsibility; or,

(2) The referral of the investigation is required by federal law or regulation or by DoD or Army regulation. See paragraph 4-12 for policy on joint investigations and paragraph 4-14 for coordination of investigations with the FBI.

b. If another agency agrees to accept responsibility for the investigation, that agency will be fully informed of the allegations and the results of the USACIDC investigation to date, if any. This may be done verbally and followed up in writing.

c. If the other agency declines to accept the responsibility for conducting the investigation, the USACIDC unit will continue the investigation or terminate in

accordance with paragraph 4-17, if applicable, or seek guidance from higher headquarters.

d. If the other agency accepts the responsibility for conducting the investigation the USACIDC unit will:

(1) Dispatch to the other agency a completed letter of referral, CID Form Letter 21-R. Delivery to the other agency is accomplished by providing the letter directly to the representative of the other agency or by forwarding it through the mail. (See figure 4-3).

(2) In the case of a (2) above, prepare an initial/referred or status/referred ROI, as appropriate, with a summary of the investigation to date and a statement that the other agency has assumed responsibility for the investigation.

(3) Discontinue investigative efforts, except as requested by the other agency to support its investigation or as directed by higher USACIDC authority.

e. If the USACIDC essentially terminates investigative efforts, the unit will, in the case of a (2) above:

(1) Establish a suspense to inquire as to the availability of the final report of the other agency every 90 days until the report is received. Entries into the AAS by agents/investigators/supervisors every 10 days are not required. Entries are required only pertaining to the suspense action every 90 days or actual investigative actions completed.

(2) Submit a final referred ROI upon notification by the other agency that their investigation has been completed. Efforts should be made to obtain a copy of their report for enclosure in the referred ROI. If the other agency's report is unavailable or cannot be obtained, the other agency's investigative results may be recorded. If the results will not be available for a considerable length of time, report all available information in the final referred ROI and submit a supplemental report when the final results are received from the other agency.

(3) The other agency's report will be inordinately delayed, USACIDC units may prepare a final referred ROI. The results of the other agency's investigation to date will be recorded in the narrative or an AIR. The source of the information will be identified.

(4) When the information becomes available, provide a report of the action taken against the subjects of the ROI.

4-11
Classified or sensitive programs

a. The Field Investigative Unit (FIU) is responsible for investigating all criminal offenses involving classified material or designated sensitive area activities and programs within the U.S. Army. A CID field element receiving information alleging criminal activity involving classified or sensitive matters connected with a special unit or program will notify the FIU prior to the submission of any report. Prompt coordination will be made with the FIU to plan an investigative approach and ensure there is no compromise of classified information. The FIU will determine the classification level or degree of sensitivity of the information and will coordinate directly with the appropriate major command. The FIU will either assume immediate control of the investigation and prepare the ROI or provide guidance to the respective CID field element. Criteria for reporting all other unauthorized disclosures or thefts of classified information is contained in paragraph 7-10(b)(5).

b. The FIU may also investigate any lesser included offense to those listed in appendix B, AR 195-2. All other investigative responsibilities of the FIU will be performed in accordance with paragraph 3-2, AR 195-2.

c. Classified or sensitive investigations will be presented directly to the Defense Procurement Fraud Unit (DPFU), Department of Justice (DoJ), for prosecutive consideration. Legal coordination will not be conducted locally unless the DPFU determines an investigation should be referred to a local U.S. attorney or the Criminal Law Division, DoJ.

d. Classified information will only be discussed after verification of security clearance and only on an appropriately secured telephone.

4-12
Joint investigations

a. Joint investigations will be initiated by USACIDC elements when Army interests in an investigation exist simultaneously with interest of one or more external investigative agencies and a decision is reached by all agencies that a coordinated effort is essential to a successful completion of the investigation.

b. A lead agency should be designated in all joint investigations to coordinate overall investigative efforts; assign tasks; and assume reporting responsibilities, including Fraud and Corruption Tracking (FACT) reporting, if applicable. An informational copy of the FACT form should be sent to the other concerned DoD investigative agency(ies). If at least one other agency is a Defense criminal investigative organization, the lead agency should come from military service having the greatest interest or upon which the matter impacts the greatest, as determined, e.g., dollar value of contracts, potential loss, or impact upon combat readiness. If involved, the FBI will normally assume the role of lead agency. In

this case, DoJ investigative guidelines will be followed. Conflicts in determining the lead agency not resolvable at the field level may be referred to Commander, USACIDC, ATTN: CIOP-ZA, for coordination and resolution with the headquarters of the other investigative agency. When only military criminal investigative organizations (MCIO) are involved, each will normally investigate leads within its parent service.

c. When necessary, written agreements can be prepared at the beginning of any joint investigation specifying the responsibilities of each agency involved in the investigation. This agreement should include such factors as designation of lead agency, any special requirements for funding including confidential funds, and responsibility for unique reporting requirements. In negotiating this agreement, USACIDC elements will ensure they are responsible for that portion of the investigation of significant interest to the Army.

d. Upon initiation of a joint investigation, the USACIDC element involved will (regardless of what agency is the lead agency) prepare and forward initial or initial/SSI and status reports as required by chapter 7 of this regulation. The investigative summary portion of the report will include the details of the investigation and a description of the responsibilities of each investigative agency involved. If available, the ROI number(s) of the other agency(s) involved will be referenced in the initial and final reports. Upon completion of the investigation, a joint investigation ROI will be prepared in accordance with paragraph 7-21.

e. When HQUSACIDC receives notification that another Defense criminal investigative organization is conducting an investigation in which there is an Army interest, it will notify the appropriate USACIDC major subordinate command. HQUSACIDC or the USACIDC major subordinate command, as appropriate, will determine the need for USACIDC involvement. The USACIDC major subordinate command will notify the proper subordinate element and request that the investigating agency be contacted at the local level to determine the feasibility of a joint investigation. Such situations not resolved at the local level will be referred to Commander, USACIDC, ATTN: CIOP-ZA.

4-13
Collateral investigations

a. A collateral ROI transmits to recipients the results of a criminal investigation conducted by a civilian agency in which there is an Army interest but for which USACIDC did not have investigative responsibility.

b. Army reporting responsibility for such incidents is assigned to provost marshals under the provisions of AR 190-45, Military Police Records and Forms.

c. All USACIDC elements may assume the collateral reporting responsibility for any offense on a case-by-case basis when the overall interests of the Army would best be served. A collateral ROI will be prepared in accordance with paragraph 7-20.

4-14
Coordination of investigations with the FBI

The 1984 Memorandum of Understanding between the Departments of Defense and Justice, as implemented by DoD Directive 5525.7, which can be found in chapter 2, AR 27-10, Military Justice, defines the respective investigative responsibilities of the FBI and the military criminal investigative organizations. This MOU establishes three categories of coordination with the FBI (described in, a through c below) to determine primary investigative responsibility in situations where dual responsibility exists.

a. Referral. Referral of investigations to the FBI will be done in writing. Although not mandatory, it can normally be expected in this case that the FBI will exercise their authority to assume primary investigative responsibility. The FBI will attempt to make this determination within one working day of receipt of the referral. Under the terms of the MOU, certain offenses other than those listed below may be referred to the FBI; however, it is USACIDC policy that those violations will b e brought to the attention of the FBI through the conference or notification methods. The following will be immediately referred to the FBI:

(1) Allegations of bribery or conflict of interest (violations of 18 USC sections 201, 203, 205, 208, 209 or 219) against present, former, or retired general or flag officers; civilians in grade GS-16 or higher; members of the Senior Executive Service (SES) or the executive level.

(2) Federal crimes, other than those described in (1) above, committed outside a military installation by persons subject to the UCMJ, but which have no connection with the person's official duties and which are not normally tried by court-martial.

b. Conference. A "conference" will be arranged with the appropriate U.S. attorney or assistant U.S. attorney with advance notification of the conference being provided to the appropriate office of the FBI. Investigative responsibility between the USACIDC and FBI will be determined at this meeting. The conference method will be utilized in the following situations:

(1) Allegations of bribery or conflict of interest involving DoD employees or DoD contractors or subcontractors (other than those allegations included in a(1) above and not to be otherwise disposed of under UCMJ.

(2) Frauds against the Department of Defense and theft or embezzlement of U.S. Government property by persons not subject to UCMJ.

c. Notice. "Notice" is an advisement to the FBI that the military has initiated an investigation into allegations of criminal acts. In the case of "notice," the FBI may exercise its authority to assume investigative responsibility, but normally should not be expected to do so. Notice will be used in the following situations:

(1) Crimes, other than those included in a and b above, committed on a military installation by persons not subject to the UCMJ, if the offense falls within the prosecutorial guidelines of the local U.S. attorney (the U.S. attorney may relieve local military investigative agencies of this reporting requirement).

(2) Federal crimes, other than those included in a and b above, committed outside of a military installation by persons subject to the UCMJ even though the offenses are normally tried by court-martial, and if the offense is within the prosecutorial guidelines of the local U.S. attorney (the U.S. attorney may relieve local military investigative agencies of this reporting requirement).

(3) Investigations involving any element of organized crime. This notification will include any information gathered concerning traditional (La Cosa Nostra) or non-traditional organized crime.

d. Referral of investigations of fraud against the Department of Defense and theft or embezzlement of government property to the DPFU in accordance with chapter 10 will satisfy the requirements for conference or notice. Acceptance or declination of an investigation by DPFU will constitute action by the Department of Justice with respect to that investigation.

e. If it appears that the Department of Justice may assume investigative responsibility and/or prosecutorial jurisdiction, and such is not in the best interests of the Army or military justice, the assistance and presence of the supporting Staff Judge Advocate should be obtained at any conference with the U.S. attorney. The Staff Judge Advocate will be able to present legal issues mitigating in favor of the Army.

f. The USACIDC units will make maximum utilization of the conference and notification methods of coordination with the Department of Justice and its investigative organizations. The USACIDC units will conduct investigations covered by those methods unless a U.S. attorney directs otherwise or the FBI makes a positive assertion of its investigative authority. When the FBI undertakes an investigation in which there is an Army interest, it should be undertaken as a joint investigation with USACIDC participation.

g. Questions concerning the types of coordination to be affected with the DoJ in any particular case should be referred to the major subordinate command staff judge advocate.

4-15
Documentation of Department of Justice declination to Prosecute

a. A declination to prosecute by a United States attorney or other Department of Justice (DoJ) component does not necessarily mean a case lacks merit to consider or proceed with other available criminal (UCMJ), civil, contractual, or administrative remedies. A DoJ declination to prosecute does not limit military or other DoD authorities from pursuing other remedies. Accordingly, where federal prosecution has been declined by DoJ, the CID investigator will ensure that prosecutive declinations by the DoJ are recorded in a manner that encourages other such remedies as may be appropriate in the particular case.

b. Military commands, DoD and DA agencies may initiate administrative, contractual, or civil action prior to the DoJ making a determination of the prosecutive merit of a particular investigation. In accordance with DoD Directive 7050.5 (Coordination of Remedies for Fraud and Corruption Related to Procurement Activities), if such action is based in whole or part on evidence obtained during a CID investigation, advance knowledge of the intended action must be provided to the investigating USACIDC unit. This requirement is not intended to delay the initiation of such action, but rather to ensure there is no adverse impact on possible criminal prosecution. (See also paragraphs 4-29, 7-14h, and 7-31).

c. Where it is the practice or intent of a United States attorney or other DoJ component to issue a written declination, investigators shall seek the inclusion of a statement similar to those listed below, when appropriate. The assigned investigator should be prepared to assist the prosecutor in preparing the specific written statement. This may include the preparation of a draft statement, if so directed by the prosecutor. The written declination will be listed as an exhibit in the interim ROI and final ROI. It will be referenced in the prosecutive status section of the final ROI.

(1) The facts evidence a degree of criminal misconduct on the part of (subject(s)). However, the case does not meet the United States attorney's standards required for federal prosecution. This declination should not be construed by your agency or command in such a way as to preclude consideration of other available criminal, civil, contractual, and administrative remedies. It may be appropriate for your agency or command to consider initiating other available remedies. These remedies should be discussed with the civilian or military attorneys assigned to your agency or command."

(2) "The facts as developed to date do not merit criminal prosecution against (subjects(s)) by this office because (reason of declination). This declination should not be construed by your agency or command in such a way as to preclude consideration of criminal, civil, contractual and administrative remedies. The facts are sufficient to warrant consideration of these or other available remedies and they should be discussed with the civilian or military attorneys assigned to your agency or command."

d. Where it is not the practice or intent of a United States attorney's Office or other DoJ component to issue a written declination, the following information will be included in the status section of the ROI.

(1) The name and title of the attorney making declination.

(2) The name of the special agent(s).

(3) Method of coordination (by telephone, correspondence, or in person).

(4) Basis for declination and fact that the declination should not be construed to preclude consideration of other available remedies. The wording should be similar to the paragraph listed in c, above.

e. The provisions of this section apply only to

(1) "Significant" EC cases (See paragraph 4-39).

(2) Any EC case involving a DoD contractor.

4-16
Early/immediate case closure

a. Early termination of USACIDC investigations is authorized in cases addressed under paragraph 4-17, where the conduct of the investigation has failed to produce any logical suspects or leads and continuation would be of little or no value in developing suspects, leads, or the recovery of property.

b. Early termination must be judiciously exercised and approved by the special agent-in-charge, operations officer, or commander.

c. Completion of early/immediate termination reports will be documented via the Final C format, as prescribed in paragraph 4-17c.

4-17
Termination of Reports of Investigations (ROI)

a. A criminal investigation may be terminated prior to exhausting all investigative leads, and a Final (C) ROI prepared when the USACIDC investigative resources could be better employed on other investigations, and when one of the following situations exists:

(1) In overseas areas, when the personnel involved as subjects are local or third country nationals or non-DoD affiliated civilians, and the local foreign country prosecutor has determined that under local law there is probable cause to believe that the subjects committed the offenses.

(2) Probable cause exists to believe that a certain person committed the offense, and that person is deceased, and it is unlikely that further investigation would result either in the addition or deletion of subjects or offenses. Also, whenever it is determined during the investigation of a death that the subject died of natural causes or accidentally caused his or her own death, the investigation may be terminated (See (9) below). However, all investigative effort expended will be reflected in the final ROI (e.g., photos, autopsy report, etc.).

(3) All of the subjects have received nonjudicial punishment or have been tried by courts-martial or in civilian criminal court for the offense(s) under investigation (or for a lesser included offense), and it appears unlikely that further investigation would identify additional subjects or would produce evidence which would exonerate an already identified subject.

(4) The supported staff judge advocate or prosecutor is of the opinion that sufficient admissible evidence is available to prosecute the subject for the offense(s), that additional investigation would produce only cumulative and unneeded evidence, and that the identification of additional subjects or offenses is unlikely. An example of such a situation is one in which numerous persons witnessed an aggravated assault and those interviewed have so consistently reported the facts that the facts are clear. Care must be taken in such instances to ensure that those interviewed constitute a reasonable cross section of the witnesses.

(5) The complainant/victim's cooperation is necessary for the satisfactory resolution of the investigation, and such cooperation is not forthcoming. If cooperation cannot be gained after reasonable effort (e.g., investigation of a self-admitted subject who refuses to provide specific information as to the alleged illegal activities, associates, places), the investigation may be terminated.

(6) A USACIDC commander, operations officer, or special agent-in-charge (SAC) of a USACIDC unit, determines that furtherance of the investigation would be of little or no value or leads remaining to be developed are not significant.

(7) When a thorough investigation fails to produce any logical subjects and there is no serious injury and/or substantial loss of government or personal property.

(8) In a death investigation when the following determination can be made:

(a) medical authorities determine that death resulted from natural causes and there is no evidence to contradict their findings or

(b) the death resulted from an accident and it is clear that no criminal act was involved.

(9) The subject is a member of another U.S. military service and that member's service investigating agency accepts the investigation.

(10) When an AUSA or DPFU determines that pursuit of the leads are not required for prosecution and the data from those leads is not needed to independently support office of the Judge Advocate General (OTJAG) suspension/debarment act ions, other administrative actions, or civil recovery.

(11) Cases may be finalized due to secrecy requirements, Rule 6(e), Federal Rules of Criminal Procedure, only after the supported SJA has been consulted. See, however, paragraphs 4-29 and 7-15e.

(12) If an action commander or prosecutor indicates intent either to take no action against the subject or take action amounting to less than a court proceeding and no further investigative assistance of CID is required by the commander or prosecutor. Furthermore, probable cause to list the subject for the listed offenses must exist. Termination of an investigation under these circumstances must be approved by a CID supervisor.

(a) In those unusual situations in which the commander or prosecutor is overruled or changes his mind and decides to request a court proceeding and the investigation has been closed, additional investigative activity should be conducted if necessary and a supplemental ROI prepared.

(b) Continuance of an investigation is not precluded regardless of the commander's intent if the USACIDC feels it warranted or a greater Army interest exists.

(13) When a United States attorney declines to prosecute any of the subjects under investigation and the affected command anticipates taking no civil,

administrative, or military judicial action. In this case, a declination will be obtained from the U.S. attorney in accordance with paragraph 4-15.

b. Any decision to terminate investigative leads will be made entirely within USACIDC channels. The decision will not be based upon directions or pressures from person(s) outside of the USACIDC. When making this decision, CID supervisors will ensure that all significant leads relating to an investigation have been developed, and that valuable investigative resources and time are not needlessly expended. To accomplish this, CID supervisors will consider the following points and exercise careful consideration and sound judgment to bring the investigation to a logical and practical conclusion:

(1) Available resources.

(2) Potential impact of the investigation on the Army.

(3) The number of subjects developed in the investigation.

(4) The nature of the allegation and the seriousness of the incident or crimes involved.

(5) The severity of injury to the victim(s) involved.

(6) The dollar amount of loss to the victim.

(7) Whether continued development of existing leads would be likely to produce only cumulative evidence.

(8) The relevancy of leads remaining to be developed to the offense under investigation.

(9) The potential for solution or recovery of property.

c. All final ROIs prepared under the provisions of this paragraph will be identified by placing a "(C)" after the report designation. The status section of the final report will include the basis for terminating the investigation. The basis f or terminating the investigation will include the specific citation in this regulation under which the case is closed and a general summary of those investigative leads that will not be pursued.

d. USACIL will be notified to terminate any examinations being expeditiously conducted on cases which will be terminated in accordance with the foregoing paragraphs.

4-18
Preparation

A USACIDC unit will not prepare military police reports (MPR) (DA Form 3975).

4-19
USACIDC use

When an MPR is received from the military police it will be filed in the appropriate case file. When a copy of the MPR is not readily available, an AAS entry is sufficient to verify that the provost marshal was notified of the USACIDC investigation. The MPR number will be documented in the Case Information section of ACIRS. An MPR provided to the USACIDC for criminal intelligence purposes only will be filed in the appropriate raw data file.

4-20
Fugitive deserter ROI

a. If the subject and/or victim of the investigation has been interviewed and all other significant leads have been accomplished when the subject/victim become a deserter, then the ROI can be terminated as a Final or terminated as a Final "C", under the provisions of paragraph 4-17(a). Whenever a final report cannot be written while the subject or victim has not been interviewed and is in a fugitive status, and all other investigative requirements have been completed, a Final "D" ROI will be prepared and forwarded to the USACRC. Leads remaining to be developed upon the deserter's return to military control will be fully detailed in the leads section of the report.

4-21
Evidence in a Fugitive Deserter ROI

a. Physical evidence will be retained by the originating office until the Final (D) ROI leads have been completed and the requirements of AR 195-5 are complied with.

4-22
Return of fugitive deserters to U.S. Army control

When advised by competent authority (e.g., civil police, FBI, military personnel office) that the subject has been returned to military control, the USACRC will forward a copy of the Final (D) ROI to the nearest USACIDC unit to facilitate the completion of the investigation. This copy will be processed as a request for assistance by the receiving unit. The gaining USACIDC unit will effect

coordination with the gaining unit commander and provide the gaining unit with a copy of the ROI. The USACRC will also forward a copy of the Final (D) ROI to the originating USACIDC unit along with a cover memorandum reflecting the USACIDC unit that received the request for assistance copy of the report. If the originating unit still has a file copy, only the cover memorandum need be sent. The USACRC will also telephonically contact or transmit an electronic message to the receiving and originating units to immediately alert them that the reports are being forwarded.

4-23
Reopening Final (D) ROI

a. When a Final (D) ROI is returned by USACRC along with the data necessary for further investigation, a supplemental report using the status report format or the SSI status report format, as appropriate, will be prepared within five business days, or by COB of the following business day in cases where the ROI is SSI reportable, after the need such reports is identified by the originating USACIDC unit.

b. The investigative summary of this supplemental ROI will report the receipt of the information causing the return of the ROI and any significant investigative activity subsequent to receipt of the ROI.

c. Each report will be sequentially numbered beginning with 1st Supplemental Report.

d. The same reporting cycle, reporting and distribution requirements for initial, status, and final ROI apply to supplemental reports. When exhibits need to be forwarded to CRC and investigative activity has been completed, a supplemental report will be prepared using the "final" report format.

e. See paragraph 8-14, for distribution criteria concerning persons in a fugitive deserter status.

4-24
ROI involving units participating in selected field training exercises (FTX's) and contingency operations

a. A separate block of ROI case numbers will be assigned by the CRC for use in controlling criminal investigations involving personnel or units participating in certain FTX's (e.g., Reforger, Bright Star) or in the execution of limited contingency plans (e.g., Grenada).

b. If a separate unit, with a unique USACIDC unit number is activated for the exercise or contingency operations, that unit will have its own ACIRS database. If the unit is deactivated at the conclusion of the exercise or contingency operations, its database, in its entirety, may be moved to any other database host. The cases would retain their original case numbers. Control of individual cases may be transferred to any other USACIDC unit using the control transfer procedures cited in paragraph 4-9. The originating office will include a copy of the documentation contained in their case file (AAS, notes, CID forms 44, etc.) as an enclosure to the memorandum of transmittal.

4-25
Sensitive investigations

All murder, rape and command monitored investigations require face-to-face coordination with the supporting SJA. Investigations involving senior personnel require special handling as described in paragraphs 5-4a and 8-40.

4-26
Inspector General reports

ROI containing IG documents or information have limited distribution, and will be handled in accordance with paragraph 8-2e.

4-27
Requests for information/records from the National Personnel Records Center (National Archives) and Army Reserve Personnel Command (AR-PERSCOM)

a. CID elements will not request records from the National Archives or AR-PERSCOM for other agencies, to include civilian law enforcement agencies, unless the request is in support of a joint ROI. The accounting and release procedures for information to non-DoD agencies are different than the procedures for release to CID, or other internal DoD agencies. Civilian law enforcement officials desiring to obtain information from AR-PERSCOM will be provided the information in paragraph b. Civilian law enforcement officials desiring to obtain information from the National Archives will be provided the information in paragraphs e and f.

b. Routine CID requests for records maintained by the National Archives or AR-PERSCOM will be submitted directly to AR-PERSCOM via the most efficient and expeditious manner available. Such requests should be forwarded to:

COMMANDER, AR-PERSCOM
ATTN: ARPC-CIS-PP (SFC Barbara Evans)
1 Reserveway, St. Louis, MO 63132-5200

Commercial..... 314-592-0620/0621
DSN.....……..... 892-0620/0621
FAX.....……..... 0628

c. When the need for National Archives or AR-PERSCOM records for a CID investigation is an emergency, a request for assistance may be forwarded to the St. Louis Fraud Resident Agency. Only true emergency requests will be accepted:

RESIDENT AGENT IN CHARGE
SAINT LOUIS FRAUD RESIDENT AGENCY
MPFU USACIDC
PO BOX 200007
SAINT LOUIS MO 63120-0007
mail175%cid175@knox-acirs.army.mil

Commercial.....314-263-XXXX
DSN..... .....…….693-XXXX
Resident Agent-in-Charge.....1873/1874
FAX.....1105

d. Requests for assistance in the St. Louis area not involving the National Archives or AR-PERSCOM requests will be forwarded to the Fort Leonard Wood Resident Agency or the appropriate Defense Criminal Investigative Organization (DCIO) IAW the Inter-agency Investigative Support Memorandum of Agreement addressing investigative support among the DCIOs.

SPECIAL AGENT IN CHARGE
FORT LEONARD WOOD RESIDENT AGENCY
6TH MILITARY POLICE GROUP (CID) USACIDC
BLDG 1907
FORT LEONARD WOOD, MO 65473-5830
mail045@acirs.wood.army.mil

Commercial..... 573-596-XXXX
DSN.....581-XXXX
Special Agent-in-Charge.....0273
Duty Agent.....0273
Answering Device.....0273
MP Desk..... 6141
FAX..... 0272

e. Local/state/Federal law enforcement agencies or prosecuting attorneys requesting records whether routine, emergency or for court “authenticated records,” must contact the National Personnel Records Center directly as follows:

(1) Requests should be on official department or office letterhead signed by a supervisor.

(2) The requests should contain as much identifying information on the subject as possible to include full name, SSAN, date of birth, place of birth, branch of service, approximate dates of service, etc.

(3) The requests should be as specific as possible as to the information requested (i.e., dates of service, assignments, awards, schools, performance appraisals, etc.).

(4) Requests should be mailed to:

National Personnel Records Center
(Military Personnel Records)
9700 Page Avenue
St. Louis, MO 63132-5200

or facsimiled to:
(314) 538-4175

(5) The request for “authenticated records” must be accompanied by a court order, warrant or subpoena with the specific information as stated in e(2) and (3) above.

(6) Email requested cannot be accepted in accordance with 5 USC 552a.

(7) Email inquiries concerning general information and request procedures can be directed to MPR.center@nara.gov.

f. Many federal investigative agencies have their own representatives at the National Records Center to handle requests by their respective agencies.

4-28
Criminal investigative support for suspension and debarment

To effectively support the Army's suspension and debarment authority, all USACIDC field operating elements will:

a. Ensure compliance with paragraphs 4-15 and 8-25.

b. Prepare an interim report of investigation if the matter under investigation is to be presented to a federal grand jury. See paragraph 7-15e.

c. Ensure certified court related documents, e.g., indictments, convictions, complaints, and judgments, are provided to the supporting Procurement Fraud Advisor and forwarded to the Army Procurement Fraud Division, U.S. Army Legal Services Agency, ATTN: JALS-PF, 901 N. Stuart Street, Suite 500B, Arlington, VA 22203-1837

d. Be prepared to provide additional assistance, as necessary, in support of suspension and debarment procedures.

e. Provide criminal history information support to local contracting officers during pre-award surveys, when requested.

4-29
Violations by USAREC personnel

a. Any USACIDC units receiving criminal complaints against personnel assigned to recruiting duties will take the following actions:

(1) Initiate a sequence number action.

(2) If any offense for which the USACIDC has investigative responsibility other than Article 84, 92, or 107, UCMJ, as they pertain to effecting an unlawful or fraudulent enlistment appears to be involved, the inquiry/investigation will be conducted as with any other complaint, and include the Article 84, 92 and/or 107 UCMJ violation(s). The USAREC Liaison Officer (LNO) will be included as an information addressee on each ROI submitted in accordance with paragraph 8-12.

(3) If the only apparent offense is a violation of Articles 84, or 92 or 107 UCMJ, as they pertain to effecting an unlawful or fraudulent enlistment, dispatch a message describing the substance of the allegation and the sequence number to USAREC LNO, 280th MP Detachment (CID), 3d MP Group, USACIDC, Fort Knox, KY 40121- 5580.

(4) If the only apparent offense is a violation of Articles 84, 92, or 107 UCMJ, as they pertain to effecting an unlawful fraudulent enlistment, the sequence number action will be maintained in an open status until instructions are provided by the USAREC LNO or higher headquarters either to complete the sequence number action or initiate an ROI.

(5) Prior to the preparation of a final ROI involving a violation of Articles 84 and 107 pertaining to effecting an unlawful or fraudulent enlistment, coordination will

be made with the appropriate USAREC brigade SJA. Telephonic coordination is authorized. This requirement is in addition to the requirement for coordination with the local SJA.

(6) A special distribution scheme for ROI pertaining to USAREC personnel is provided in chapter 8, paragraph 8-12.

b. Upon receipt of notification from a USACIDC unit, pursuant to paragraph 4-29a(3), the LNO will:

(1) Initiate a sequence number action.

(2) Inform USAREC.

(3) Determine, in coordination with USAREC, whether USAREC can adequately inquire into the allegation or whether an investigation by the USACIDC would be more appropriate.

(4) Inform the reporting USACIDC unit by message within five working days to either complete its sequence number action or initiate an ROI.

c. When the inquiry into an allegation of a violation of Article 84, 92, or 107 UCMJ, pertaining to effecting an unlawful or fraudulent enlistment is conducted by USAREC without investigation by the USACIDC and results in a relief of a recruiter, the LNO will:

(1) Ensure that a copy of the result of the USAREC inquiry is received.

(2) Review the USAREC report to determine whether it reflects an apparently thorough development of the facts and whether there are indications of other crimes for which the USACIDC has investigative responsibility.

(3) If the review of the USAREC ROI identifies a requirement for a USACIDC investigation of other serious criminal offenses, initiate a USACIDC ROI or if appropriate, forward the USAREC ROI to the USACIDC office having investigative responsibility for the area where the additional criminal offense(s) took place or where the suspect(s) reside and request that office to initiate a USACIDC ROI.

(4) If the review of the USAREC ROI does not reveal a need for additional investigation by the USACIDC, initiate and prepare an initial/Final USACIDC ROI. The Initial/Final USACIDC ROI should be prepared in Collateral ROI format and will include a copy of the USAREC ROI as an attached exhibit. The decision to list USAREC personnel as ROI subject(s) for a recruiting impropriety will be based upon credible information standards and in compliance with DODI 5505.7.

(5) Provide a copy of the USACIDC ROI to HQ, USAREC, ATTN: RCRO-RI. Since action taken against subject(s) will already be reported in the USAREC ROI, the use of DA Form 4833, Commander's Report of Disciplinary and/or Administrative Action should not be necessary. The results of the action taken will be reported in the USACIDC ROI.

(6) If the review of a USAREC ROI does not reveal any other serious criminal offense(s), but does address offense(s) within PMO investigative responsibility, coordinate with the local PMO and pass on the information for action as deemed appropriate.

d. Upon receipt of notification from HQ USAREC of allegations of other serious criminal offenses against USAREC personnel for which the USACIDC has investigative responsibility, the LNO will:

(1) xxxxxx

(2) Coordinate with USAREC to verify the reported offense(s) fall within the investigative responsibility of the USACIDC.

(3) If a USACIDC investigation is required, forward the information to the appropriate USACIDC unit by Memorandum of Transmittal for initiation of a ROI.

(4) The LNO will monitor the progress of the USACIDC investigation of the USAREC recruiter(s) which have been in an open status more than 90 days and respond to inquiries from USAREC pertaining to those investigations.

e. The USACIDC units will strive to complete investigations involving recruiters within 90 days. Any Request for Assistance (RFA) involving recruiters will be completed within five working days, if possible.

4-30
Violations by health care providers

a. Headquarters, USACIDC, will be notified of all allegations of misconduct involving health care providers as a subject or suspect.

b. Health care providers are defined as military or civilian personnel who, under military regulations, are credentialed to provide patient care in military medical and dental treatment facilities or those enrolled in training programs leading to qualification in a medical or dental specialty that requires credentialing. This includes, but is not limited to, physicians, dentists, chiropractors, registered nurses, dental hygienist, etc.

c. Misconduct which must be reported includes any improper, unethical, or unprofessional conduct not in keeping with that expected or required by health care providers. It includes:

(1) Violations of those Articles of the UCMJ which carry a maximum punishment of confinement for a period of one year or more.

(2) Any act involving moral turpitude.

(3) Conduct constituting an abuse or exploitation of a patient arising out of the trust and confidence placed by the patient in the health care provider.

(4) Conduct or treatment not meeting generally accepted standards of quality patient care.

(5) Malpractice.

d. One copy of all initial, status, final, supplemental ROIs and reports of action taken or the lack thereof, involving health care providers as suspects/subjects for any incident discussed above will be provided to Commander, USACIDC, ATTN: CIOP-ZA.

e. This is not to be construed as an expansion of the investigative thresholds or responsibilities of USACIDC as defined in AR 195-2. Only those incidents which fall within USACIDC's investigative purview will be reported in accordance with procedures outlined above.

4-31
Internal Revenue Service (IRS)

a. All CID special agents are authorized to initiate the release of investigative information for law enforcement purposes to the IRS. Such releases may be in the form of entire reports or as summaries and extracts, depending upon the sensitivity of the information and the need to protect the source. There are two broad categories of information which CID should refer to the IRS:

(1) Information indicative of violations of U.S. tax law should be reported to the IRS. The IRS is generally interested in illicit income in any amount but will consider prosecution of those cases involving unreported income of substantial amounts. Such cases are reported to the Criminal Investigation Division of the local IRS district office. Consider for referral all cases where substantial income is the result of such activity as drug sales, black-marketing, theft, diversion of property, bribery, etc. Documenting release of entire reports or fragments will be made in accordance with AR 27-40 and chapter 21 of this regulation.

(2) Information indicating non-compliance with tax laws by persons over a large geographical area, such as a general assessment of widespread black-marketing in several overseas countries, or an investigation of widespread corruption in a specified organization, should also be reported to the Criminal Investigation Division of the local IRS district office or the IRS representative located at most U.S. embassies.

b. The IRS maintains files containing tax-related information on U.S. citizens, resident aliens, and businesses. This information should not be overlooked as a potential source of personal or corporate financial data in CID investigations. The disclosure by the IRS of tax information to federal officers or employees for administration of non-tax related federal criminal laws is governed by section 6103(i) of the Internal Revenue Code (IRC) (Title 26 USC). The two general categories of in formation available are "returns" and "return information."

(1) A "return" is any tax return, information return, declaration of estimated tax, claim for refund required by, provided for, or permitted under, the provisions of the Internal Revenue Code which is filed with the IRS by, on behalf of, or with respect to any person. It includes any amendment or supplement to a return, including supporting schedules, attachments, or lists which are supplemental to, or part of a return.

(2) "Return information" is a taxpayer's identity (including name, mailing address, taxpayer identification number, or a combination thereof), the nature, source, or amount of his/her income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over-assessments, or tax payments. Also, whether the taxpayer's return was, is being, or will be examined, or subject to other investigation or processing, or any other data received by, recorded by, prepared by, furnished to, or collected by the IRS with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount of liability) of any person under the Internal Revenue Code for any tax, penalty, interest, fine, forfeiture, or other imposition or offenses. For purposes of section 6103(i), the term "return information" is separated into two distinct categories:

(a) "Taxpayer return information" - Return information filed with or furnished to the IRS by or on behalf of the taxpayer to whom such information relates.

(b) "Return information" (other than taxpayer return information) - return information which is not provided to the IRS by or on behalf of the taxpayer (i.e., information obtained from a third party who is not the taxpayer's a gent or representative).

The important point to remember is that any information provided to the IRS by the taxpayer or on behalf of the taxpayer will require a court order for release. Information provided to the IRS by a third party, not on behalf of the taxpayer,

may be releasable by written request to IRS. Generally, information most useful to the CID will be obtainable only by court order.

c. Section 6103(i), Internal Revenue Code, lists six circumstances wherein return or taxpayer return information may be disclosed. Two of these circumstances are of particular interest to the CID.

(1) Disclosure Pursuant to Ex Parte Court Order - IRC 6103(i)(1). An "ex parte" order is a court order directing the IRS to release specified information within its files. Under this circumstance, returns and return information (including taxpayer return information) may be released to CID personnel who are personally and directly engaged in any of the following activities: preparation for any judicial or administrative proceeding pertaining to the enforcement of a specific federal criminal statute (including the UCMJ) to which the United States or such agency is or may be a party; any investigation which may result in such a proceeding; or any federal grand jury proceeding pertaining to enforcement of such a criminal statute to which the United States or such agency is or may be a party. Information disclosed for these reasons is solely for the use of the persons engaged in the above specified activities. (See figure 4-4).

(2) Disclosure Pursuant to Written Request - IRC 6103(i)(2). Disclosure of return information (other than taxpayer return information) may be made to CID personnel who are personally and directly engaged in any one of the categories o f activity (for example, investigation) listed in paragraph 4-32c(1), in response to a request to the IRS from certain officials. The CID will normally obtain requests from one of the following:

(a) The DoD Inspector General.

(b) Any DOJ attorney.

d. A CID special agent may obtain an ex parte order by submitting a request letter to a U.S. attorney. The request letter should include: the name, mailing address, and social security number of each taxpayer with reference to what material is sought; the date by which the material is needed, and, if the need is immediate, a request for expeditious handling (IRS takes about 45 days to process an ex parte order once received, it may take more time for the U.S. attorney to obtain the order), and whether the material is sought solely for investigative purposes at the time of the request or whether use of the information in a criminal judicial proceeding is anticipated. If use is only anticipated for investigative purposes and later is necessary for court, the IRS will need to be re-contacted to determine whether the information can be used by the court. Therefore, it is best for the applying official (U.S. attorney, etc.) to anticipate such use in judicial proceedings in the application and court order, if possible. Request letters may be signed by CID unit commanders or their designees. Informal coordination with the U.S. attorney's office is encouraged

before submitting a formal request. Also, consider the following factors when completing the request letter and attachment:

(1) The application for court order, which the U.S. attorney will prepare, must contain sufficient information for the judge to grant the order. Therefore, the CID request letter and attachment must contain sufficient information to establish that there is reasonable cause to believe, based upon information believed to be reliable, that a specific criminal act (violation of a federal criminal statute, including the UCMJ) has been committed; that there is a reasonable cause to believe that the return or return information is or may be relevant to a matter related to the commission of the criminal act; that the return or return information is sought only for use in a federal criminal investigation or proceeding concerning such act and the information sought cannot reasonably be obtained under the circumstances from another source.

(2) The court order, itself, will be carefully worded so the disclosure by the IRS will not extend beyond the scope of the order. Unless otherwise provided in the order, disclosure will be limited to those returns and return information within the IRS' possession on the date of the order. If the order also is intended to cover returns and related return information subsequently received or developed by the IRS for the years authorized, the order should specifically provide for further disclosures and should designate a specific cut-off date. For example, the order should provide that the IRS disclose information which may come into its possession subsequent to the date of the order, but for a period no later than XXX number of days thereafter (e.g., 60 or 90 days generally).

(3) If for some reason there is a need to protect the application and order from disclosure (typically when the ex parte order becomes a matter of public record, unless directed otherwise, IRS concurrently notifies the taxpayer that information about him/her has been released), a motion to this effect should be filed simultaneously. This action is indicated if disclosure would jeopardize the ongoing investigation. If the court grants the application, a certified copy of the order should be sent to the applicable IRS district office in the area where the taxpayer resides. If unable to identify the correct IRS office, the order is sent to the Director, Disclosure and Security Division, IRS, 1111 Constitution Avenue, N.W., Washington, DC 20224.

e. Access to return information (other than taxpayer return information) is obtained by a written request from the DoDIG or any DOJ attorney.

f. Under 26 USC 6103(i)(4), returns and taxpayer return information may be used in judicial and administrative proceedings if the information is probative of a matter in issue, relevant to the commission of a crime, or to the guilt or liability of a party. The law allows such information to be disclosed in proceedings pertaining to the enforcement of a federal criminal statute, as well as in related civil forfeiture proceedings which may be pursued in addition to or in lieu of

criminal prosecutions. Since IRS information may only be used in a few very specific non-criminal judicial or administrative proceedings, it is preferable that the concerned attorneys handle all aspects of such use. The law also states that returns and taxpayer return information may be disclosed to a defendant pursuant to the Jencks Act (18 USC 3500) and the discovery provisions of the Federal Rules of Criminal Procedure (Rule 16). With respect to disclosure of return information, other than taxpayer return information, 6103(i)(4)(B) allows disclosure in a judicial or administrative proceeding in which the United States is a party without any specific findings of relevance such as are applicable to returns and taxpayer return information. Nonetheless, 6103(i)(4)(C) prevents the admission into evidence of any return information where such admission would identify a "confidential informant" or impair a civil or criminal tax investigation.

g. The outlined procedures for obtaining returns and taxpayer return information do not apply when a grand jury investigation encompasses both Title 26 tax violations and Title 18 violations, and the IRS becomes involved. If IRS special agent s participate in the grand jury investigation and develop information in the grand jury context, they may share it with other law enforcement agency participants.

4-32
Military Intelligence (MI) coordination

a. AR 380-13 (Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations) pertaining to the acquisition and storage of information concerning non-DoD affiliated persons and organizations, does not apply to authorized criminal investigations and law enforcement information gathering activities which are the responsibility of the Military Police and the USACIDC. The fact that some USACIDC functions are exempt from the provisions of this regulation should not be used to justify the use of USACIDC special agents and/or registered sources for off-post covert MI operations. Such use of USACIDC resources may not be authorized. Close coordination with the supporting SJA or HQUSACIDC SJA should be effected prior to undertaking any such actions.

b. Every effort should be made to keep MI personnel fully aware of all information which might be of military intelligence value.

c. The Military Intelligence is concerned about subjects of ROIs who have security clearances and is especially concerned about information regarding possible terrorist involvement in any assassination, kidnapping, bombing, theft of ammunition, weapons, explosives, classified material, and the disclosure of classified information.

d. Incidents involving the actual or possible disclosure of classified information fall under the provisions of AR 381-12 (Subversion and Espionage Directed Against U.S. Army - SAEDA) and must be promptly reported to military intelligence. In formation about such incidents will at least initially be classified CONFIDENTIAL or higher as needed and will not be discussed over unsecured telephone links or sent by methods not authorized for the transmission of classified information.

4-33
United States Secret Service (USSS)

Under certain limited circumstances provided for in 18 USC 3056, the USSS may require that USACIDC special agents assist them in protecting the President of the United States and other designated officials. When so assigned, USACIDC special agents will conform to USSS regulations and directions. In addition, the USSS and the DoD are required to exchange certain types of information concerning possible threats against designated officials outlined in paragraph. 7-10.

4-34
Support by United States Marshals Service (USMS)

During some USACIDC investigations involving civilians, it may become necessary to seek the assistance of the USMS. The USMS will assist CONUS USACIDC units in serving bench warrants, arrest warrants and search warrants. Normally, the USMS discourages providing assistance in the service of summons and subpoenas; however, assistance will be provided if the USACIDC special agent anticipates violence or physical efforts to prevent service of the subpoena or summons.

4-35
Postal investigations

a. The mail within U.S. jurisdiction enjoys the protection of federal law until received by the addressee. Thefts from the U.S. mail fall within the U.S. Postal Inspector's area of responsibility, especially in the CONUS environment.

b. The local postal inspector will be coordinated with on all postal matters and thefts occurring within CONUS and in OCONUS areas which have resident postal inspector(s) present. Depending upon the facts and circumstances of a case, the investigation may be referred to the postal inspector. It may be worked as a joint investigation, or it may be left in the responsibility of the CID element concerned.

c. Because of the specialization of postal inspectors, they offer CID an extensive depth of knowledge and experience which can be drawn upon. Postal inspectors have access to computerized systems of information which allow them to chart losses to a mail operation and may tie those losses in with already established and identified groups who prey upon the postal system.

d. For CID reporting purposes, once material has been entered into the postal system, it is in the care and custody of the U.S. Government until received by the addressee. The U.S. Government (U.S. Postal Service/Military Postal Service, as appropriate) will be identified as the victim of offenses involving the theft of mail matter. The individual or business activity that mailed the item may be listed as victim also, provided that some article(s) of value have been identified as being taken from the mailed item. Normally, addressees are not considered to be the victim so long as the mail still remains in postal channels. The addressee may be listed as the victim if it can be established and shown that the theft occurred from the individually assigned mail box or receptacle of that person.

4-36
Investigative support to Defense Protective Service (DPS)

The DPS is the agency responsible for the investigation of all criminal acts occurring within the Pentagon and other designated DoD buildings located in the National Capitol Region. Based upon a memorandum of understanding between DPS and USACIDC, the DPS may submit requests for assistance to USACIDC field elements in support of felony crime or serious incidents which they investigate and which require investigative support outside of the National Capitol Region. RFAs from DPS will be made in writing, either letter or message format, and will provide sufficient facts and information necessary for the USACIDC field element to complete the action. Telephonic requests may be made for emergency or exceptional situations. The USACIDC field element receiving the RFA will furnish a written information report directly back to DPS furnishing the results of the RFA and/or the reasons the request could not be accomplished. USACIL support will also be provided when DPS submits a DA Form 3655, requesting such support. Polygraph support for investigations involving U.S. Army personnel or employees may also be requested.

4-37
Centralized Accident Investigation Ground (CAIG) Program

a. The CAIG team, based at Ft Rucker, AL, has responsibility for the investigation of class A, on-duty, non-pov accidents as defined in AR 385-40, Accident Reporting and Records, occurring in CONUS plus other selected accidents Army-wide. The team conducts safety investigations and prepares a

technical report intended for accident prevention purposes only. This report may not be used for administrative or disciplinary personnel actions.

b. As the CAIG team and USACIDC elements may simultaneously be investigating the same accident(s), cooperation to the maximum extent permitted by regulation is imperative. The CAIG is not intended to interfere with, impede, nor delay law enforcement efforts to determine criminal intent/acts. The exchange of factual information to the extent permitted by applicable regulations is highly encouraged. While the purposes of the two investigations are distinctly different, the timely accomplishment of both is in the best interest of the Army. Criminal investigations; however, have priority.

c. The CAIG team is required to establish contact with the appropriate Military Police and USACIDC offices upon arrival, maintain liaison, report as soon as possible any discovery of criminal intent/acts, and not alter or remove physical evidence without the concurrence of the law enforcement agency responsible for the scene of the incident. Likewise, law enforcement agencies are expected to cooperate with the CAIG team to the maximum extent feasible and consistent with applicable regulations. Such cooperation is especially critical with respect to the interview of victims and witnesses, and in the preservation and collection of evidence.

d. Free exchange of factual information between CAIG investigators and law enforcement agencies should be mutually beneficial and is encouraged. Factual information, such as equipment tear-down analysis reports, photographs, wreckage diagrams, witness names, etc., which are contained in CAIG technical reports will be made available to law enforcement agencies upon request. Refer to AR 385-40.

4-38
The Defense Investigative Management Information System (DIMIS)

a. The DIMIS is a centralized, automated data system designed to monitor, report, and analyze specific information from certain ROIs and the action taken against identified subjects. The DoDIG is the proponent for DIMIS policy and procedures and uses DIMIS for routine/special reports to Congress and the Secretary of Defense. DIMIS reports are normally submitted only on closed cases; however, certain exceptions exist, such as when there has been a significant subject disposition action, i.e., indictment, or a criminal or civil judicial action (conviction, judgment, or settlement). The reporting directives and instructions for DIMIS are contained in DoD Manual 5505.4M and USACIDC implementing instructions which should be consulted for specific details.

b. An ROI is DIMIS reportable if any one or more of the following exists:

(1) There is any actual or attempted loss to the U.S. Government as a result of criminal activity.

(2) The ROI involves an alleged offense of bribery, conflict of interest, conspiracy to defraud, or violations of standards of conduct whether or not there is any monetary loss to the U.S. Government.

(3) The case involves actual or estimated loss to the government from wrongful damage or destruction by mechanical or physical means, arson, or explosion.

(4) The case involves property destruction/loss or personnel injury/death arising from a known or suspected terrorist act.

4-39
Reporting of significant economic crime (EC) cases

a. Significant EC investigations are required by DoDI 5240.4 to be reported to the Secretary of Defense. For purposes of this requirement, "Significant Economic Crimes" are defined as:

(1) Allegations of fraud or theft:

(a) With a potential loss to the Government of $500,000 or more, or

(b) When the subject is:

1. An installation or ship commander, or

2. In or retired from the military grade 0-6 and above or civilian GS/GM grade 15 and above, and the potential loss to the Government is $5,000 or more.

(2) Any criminal corruption case related to procurement involving current or retired DoD military or civilian personnel.

(3) Any investigation into defective products or product substitution in which a SERIOUS HAZARD to health, safety, or operational readiness is indicated, regardless of loss value.

(4) Any criminal case, regardless of the allegation, which has received, is expected to receive, or which if disclosed could reasonably be expected to receive SIGNIFICANT media coverage.

b. Reporting is accomplished through the SSI reporting system to the Current Operations Division, DCSOPS, HQUSACIDC. As SSIs meeting the above criteria

are received from field elements, the Current Operations Division forwards the SSI through the Army Staff and DoDIG to the Secretary of Defense.

4-40
Initiation of ROIs in Deployment Situations

a. General.

This paragraph outlines a standardized policy for reporting criminal investigations during contingency operations.

b. Policy. It is a principle of this command that the reporting format for all investigations conducted by or for CID elements will be the Report of Investigation (ROI). Whenever an investigation of whatever scope (limited or full) is initiated, the results will be reported by the ROI format. AR 195-2 and this regulation identify four basic criteria that must exist to justify Army jurisdiction and responsibility to investigate crime:

(1) There must be some credible information that a crime has occurred. A preliminary inquiry may be conducted to reach the credible information standard, but once that standard is reached, an ROI would be initiated if the remaining criteria below have been met.

(2) The Army must have investigative authority to investigate. Investigative authority refers to matters in which the Army has the legal authority (jurisdiction) to conduct a criminal investigation. In a deployed environment, whether combat or peacekeeping mission, there is Army investigative authority when the supported commander requests the investigation to further the Army's mission in that area. If the Army is in support of an international entity (such as NATO or the UN), the use of investigative resources is an official act in furtherance of the Army's overall mission to support the approved objectives of the international entity. Unofficial investigations or investigations not in support of the Army mission are prohibited.

(3) There must be an Army interest in the case. In deployed situations, there is an Army interest in a criminal case when the case impacts the accomplishment of the Army's mission or capabilities and/or when it is requested by the supported commander to further the Army's mission.

(4) CID must have the responsibility to investigate (that is, the alleged crime is within our investigative purview). CID usually investigates the felony crimes identified in AR 195-2. As noted in AR 195-2, however, CID's investigative purview can be adjusted to include lesser crimes if it would serve a better or overall law enforcement goal.

c. Deployment considerations

(1) When deployed, CID agents generally find themselves in one of two types of situations -- a functioning government exists or it does not exist. The following paragraphs describe ROI initiations in these situations:

(a) Functioning Government: When the Army is deployed to a foreign country that has an established and functioning government and law enforcement system (police, prosecutors and a judicial system), the following guidance applies.

1. Authority to investigate is usually determined by international treaty or agreement (such as a Status of Forces Agreement (SOFA)), by the policies of the host government, or the U.S. ambassador. When questions arise in this area as to investigative authority, coordination should be effected with the supporting SJA or Group judge advocate. CID will not conduct any investigations (however limited or preliminary in nature) in violation of such agreements or policies.

2. CID will not normally conduct investigations concerning non-Army affiliated civilians committing crimes on other non-Army affiliated civilians or involving non-Army equipment/supplies outside Army controlled property. If requested to conduct an investigation by a field grade officer or higher because some Army interest is involved, CID will conduct a collateral or joint ROI to the extent allowed by treaty or policy and local law enforcement authorities.

3. When criminal incidents involve Army affiliated personnel (military, family member, civilian or contractor) or Army property, the conduct of collateral or joint ROIs will be accomplished to the extent allowed by treaty or policy and local law enforcement authorities.

4. When criminal incidents within CID purview occur on Army controlled property (such as an installation, kaserne or camp), or involve Army personnel, assets and/or resources on or off Army controlled property, ROIs will be conducted. The conduct of such ROIs will follow any guidelines, notifications or other limitations set forth by treaty or policy and local law enforcement authorities.

(b) Non-Functioning Government: When the Army is deployed to a foreign country that has no established (or a severely limited) functioning government and no law enforcement system (police, prosecutors and a judicial system), the following guidance applies.

1. Authority to investigate in this situation is usually determined by the Army’s mission and the requests of the senior supported Army commander (or senior U.S. commander in joint operations). When questions arise as to investigative authority and the Army’s mission, coordination should be effected with the supporting SJA or Group judge advocate. If the senior Army commander

delegates his authority, CID will respect requests from the delegatee. If the senior Army commander sets threshold criteria for investigations, CID will respect those limitations. CID will not investigate outside the authority of the senior Army commander (or senior U.S. military commander in joint operations). CID will not conduct any investigations (however limited or preliminary in nature) that are not in furtherance of the Army mission.

2. CID may conduct investigations concerning non-Army affiliated civilians committing crimes on other non-Army affiliated civilians or involving equipment/supplies outside Army controlled property, if such investigations are requested by the senior supported commander or meet some predetermined threshold criteria. Any such investigations (no matter how limited) will be reported via the ROI format. Such investigations may be finalized early if the original intent of the commander's request has been met, or if the completion of other outstanding leads is precluded by hostile fire, hostile territory, or other local adverse conditions. It is anticipated that many of these ROIs will be completed using the procedures for a Final(C).

3. When criminal incidents involve Army affiliated personnel (military, civilian or contractor) or Army property, the conduct of ROIs will be accomplished to the extent allowed by local environment and threat conditions. Final (C) procedures may be used as appropriate for these investigations.

4. When criminal incidents involving anyone occur on actual Army controlled and occupied property (such as a base camp), ROIs will be conducted. Final(C) procedures may be used as appropriate for these investigations.

d. Investigations Involving, Enemy Prisoners of War (EPW), Retained Personnel (RP), Civilian Internees (CI) and other Detainees (OD). For guidance concerning the investigation of detainee deaths see paragraph 5-24 of this regulation.

(1) AR 190-8 is a multi-service regulation that applies to the Army, Navy, Air Force and Marine Corps (OPNAVINST 3461.6, AFJI 31-304, and MCO 3461.1), and implements DoD Directive 2310.1 and DoD Directive 5100.7. AR 190-8 directs that all allegations of criminal acts or war crimes committed by or against EPW/RP/CI/OD be reported to CID.

(2) IAW 190-8, all persons captured, detained, interned or otherwise held in US Armed Forces custody will be given humanitarian care and treatment from the moment they fall into the hands of the U.S. forces until final release. It is DoD, Army and command policy that inhumane treatment of EPW, CI, RP, and OD is prohibited and cannot be justified by the stress of combat or by deep provocation. All prisoners, detainees, and internees will receive humane treatment without regard to race, nationality, religion, political opinion, sex or other criteria. IAW AR 901-8, they will be protected against all acts of violence to include rape, forced prostitution, assault, theft, bodily injury, reprisals of any kind,

insults and public curiosity. AR 190-8 specifically prohibits murder, torture, corporal punishment, mutilation, collective punishments, execution without proper trial, and all cruel and degrading treatment.

(3) Inhumane treatment is a serious and punishable violation under international law and the UCMJ. IAW AR 190-8, AR 195-2 and CIDR 195-1 (especially paragraphs 4-40a-c above), CID elements receiving allegations of felony criminal acts or war crimes committed by or against EPW/RP/CI/OD will investigate such allegations as an ROI. IAW AR 195-2, CID may adjust its normal investigative purview to include lesser crimes or misdemeanors if it would better serve the supported commander or the overall law enforcement goal.

(4) If the U.S. Armed Forces element conducts a commander's inquiry (an AR 15-6 investigation or equivalent) prior to notifying CID of an allegation involving felony criminal acts or war crimes committed by or against an EPW/RP/CI/OD, the supporting CID element will obtain a copy of and review the inquiry to determine if it thoroughly and fairly investigated the incident(s). If the US Armed Forces element did not conduct a commander's inquiry or if further investigative efforts are deemed appropriate, the supporting CID element will initiate an ROI to continue the investigation.

4-41
Reporting positive command-directed urinalysis test results

a. Regardless of the type of drug detected, a CID ROI will be initiated to investigate and index known drug offenders identified through the Army's command-directed urinalysis testing program. Exceptions may be granted as needed by Groups with notifications to DCSOPS when such changes occur. The following criterion is established for initiating CID reporting procedures:

b. A CID report of investigation will not be initiated based only upon prescreen field test results. In accordance with AR 600-85, Army Substance Abuse Program (ASAP) a confirmation of the positive finding must be provided by an authorized forensic toxicology drug testing laboratory (FTDTL) approved by the ASAP. A Medical Review Officer (MRO) must review all urine results confirmed positive by the FTDTL for opiates, amphetamines, and barbiturates. The MRO review must confirm that the individual, who provided the positive urine, has been interviewed and concludes that illegal drug use is the likely cause for the positive result.

c. A CID report may be initiated when the prescreen field test results are supported by already known information on the individual's drug usage, or when an admission of drug use has been provided by the individual concerned.

d. Multiple abusers from the same unit, consistent with the criteria above, will be jointly listed as subjects in the same report when testing positive on the same command directed urinalysis test. Separate reports listing each individual independently will not normally be initiated.

e. The positive urinalysis finding confirmed by an authorized FTDTL and a MRO provides credible information for listing an individual as a subject in an initial ROI. The subject will be listed for wrongful use of the identified controlled substance when the offense is based on urinalysis testing. Other investigative procedures normally followed in developing an investigation will be pursued, as appropriate, to obtain further corroboration of the offense(s), if possible, or to provide the individual the opportunity for exoneration. Procedures for early closure of the investigation outlined in paragraph 4-17 may be used, when appropriate.

4-42
Processing of United States Army Reserve (USAR) Personnel for Positive Urinalysis Results

a. A reservist whose urine, which was obtained while the reservist was subject to the UCMJ, subsequently tests positive for the presence of a controlled drug--in the absence of any other evidence--will not be apprehended or listed as a subject/suspect for possession or use unless, given the metabolism period of the drug testing positive, probable cause exists to believe the drug was ingested during a period of UCMJ status.

b. Therefore, a positive urinalysis based upon a urine sample collected over a weekend drill (inactive duty for training or IDT) is an insufficient basis in and of itself to apprehend or list as a subject/suspect because this fact fails to establish that the substance was consumed while in a UCMJ status. Proof that the reservist merely used illicit drugs at some time [as opposed to a time of UCMJ status] is insufficient for either apprehending or listing purposes by military authorities because the burden of proof is on the government to show probable cause existed to believe the illegal use occurred at the time the suspect was subject to the UCMJ.

c. The USACIDC has the right to conduct a preliminary inquiry to determine the circumstances surrounding the positive urinalysis, to include questioning the suspect and potential witnesses. Information concerning the positive urinalysis and the results of any preliminary inquiry should also be passed to the appropriate military intelligence unit. A positive urine test along with a confession, damning eyewitness testimony, or other sufficient evidence of use while in a UCMJ status could support apprehension and/or listing the reservist as a subject/suspect. Further, if the reservist were visibly impaired and could not properly perform IDT duties, incapacitation for performance of duties, Article 134, UCMJ, might be an appropriate offense.

d. If a reservist performs annual training and on the fourth or subsequent day provide a urine sample which tests positive for drugs, the suspect could be apprehended and listed as a subject for use because given the metabolism period, the conclusion may properly be drawn that the subject probably consumed the drug during a period of UCMJ status. The following usual time periods must elapse after drug use for there to be a negative result:

(1) Marihuana: 48-72 hrs for one time use;

(2) Cocaine: 48-72 hrs for one time use;

(3) Amphetamines: 24-72 hrs.;

(4) Barbiturates: 24-72 hrs;

(5) Morphine: 48-72 hrs;

(6) Phencyclidine: (PCP): 24-l68 hrs;

(7) LSD: 6-l8 hrs.

The reservist must be in a UCMJ status for a length of time longer than these metabolism periods, if apprehension/titling is to be based solely upon positive urine test results.

4-43
Procedures involving incidents of obtaining services (telephone services) under false pretenses

a. The USACIDC will only investigate incidents of obtaining telephone services under false pretense of a value of $1,000 or more. The value of $1,000 is the aggregate amount of telephone services illegally obtained by a single subject and not the individual victim's loss (telephone company and subscriber). For example, PVT SMITH is in receipt of a monthly telephone bill/statement and discovers that numerous telephone calls have been billed to his/her account, which he/she did not make, and the amount of the bill/statement is $1,000.00. Subsequently, the telephone company identifies 20 separate individuals making these telephone calls and each is responsible for $50 of the total amount of the bill, or 2 individuals are identified and each responsible for $500 of the total amount of the bill. In neither of these two examples would the responsibility for investigation fall within the USACIDC purview.

b. A report of investigation involving telephone services will not be initiated unless there is an Army interest, occurred on an installation or location under the control of the Army, and is within the investigative purview of the USACIDC.

c. On a case-by-case basis, USACIDC may investigate incidents of obtaining telephone services under false pretenses that have not met the aforementioned criteria when deemed appropriate and after considering the totality of the circumstances.

4-44
Intelligence-related investigations

a. The USACIDC is the sole agency within the Army responsible for the investigation of felony crimes (except for those crimes as prescribed by AR 195-2 and AR 190-30, Military Police Investigations). Therefore, an intelligence-related felony crime associated with espionage is within the investigative purview of the USACIDC. When the MI notifies a USACIDC investigative unit with credible information to believe a felony intelligence-related crime has been committed, the USACIDC unit will initiate appropriate investigation procedures in accordance with USACIDC policies, and will work jointly with the MI to investigate the matter to serve Army and national interests. If a USACIDC unit initiates an investigation concerning an intelligence-related crime unbeknownst to the MI, the USACIDC unit will notify the nearest MI unit and request that they join the investigation.

b. To further a better working relationship between the USACIDC and the MI, the Current Operations Branch, HQUSACIDC, will conduct routine liaison with the Army Central Control Office, U.S. Army, Intelligence and Security Command (INSCOM). See Paragraph 8-45 for distribution of joint investigations with Military Intelligence.

4-45
U.S. Soldiers' and Airmen's Home

a. Responsibilities:

(1) The Commanding General, USACIDC, agrees to provide access to USACIDC investigative facilities and resources, on a non-reimbursable basis, and as resources permit, for the following categories of services:

(a) Criminal investigative laboratory support.

(b) Criminal investigative polygraph support.

(c) Requests for records checks of the National Personnel Records Center, St. Louis, MO, through the St. Louis Branch Office, USACIDC.

(d) U.S. Army Crime Records Center checks.

(e) Requests for assistance (RFA) to USACIDC field elements.

(f) Major crime scene processing support.

(g) Legal coordination for the obtaining of subpoenas, search warrants and authorization for wire or oral communication intercept.

(2) The Director, USSAH, agrees to comply with policy and procedures outlined in applicable USACIDC and Department of the Army regulations concerning the preparation of various written requests for the categories of services provided and to comply with applicable directives which apply to the protection and release of investigative information obtained.

b. Procedures:

(1) Requests by criminal investigator(s) or other officials of USSAH for investigative services agreed upon in paragraph 4-45a will be prepared in accordance with CID Regulation 195-1 and other appropriate directives.

(2) The USSAH criminal investigator(s) will coordinate directly with the USACIDC office from which the service is requested.

(3) The Deputy Chief of Staff for Operations, Headquarters, USACIDC, and the Chief, Security and Investigations Division, USSAH, will serve as points of contact for implementation of this agreement.

4-46
Hate Crimes Investigations

a. For USACIDC purposes only, a hate bias crime is defined as "A criminal offense against a person or property which is motivated, in whole or in part, by the offender's bias against the actual or perceived race, color, religion, national origin, ethnicity, gender, disability, or sexual orientation of any person."

b. Upon notification of any incident or allegation, whether it is within normal USACIDC investigative purview or not, that involves either an actual or suspected hate crime, USACIDC elements will conduct a preliminary investigation. The only exceptions are hate bias graffiti and provoking speeches/gestures as described below.

c. If during the course of the preliminary investigation, a determination is made that the incident involved a hate crime, the following steps will be followed:

(1) If it is determined that the reported incident involves a hate crime and is within the normal investigative purview of USACIDC, the incident will be investigated and reported as an ROI/SSI.

(2) If it is determined that the reported incident involves a hate crime, but is not within USACIDC's investigative purview, the local USACIDC supervisor has the discretion to retain investigative purview. If the investigation is retained by USACIDC, it will be investigated and reported as a ROI/SSI. If the investigation is referred to the military police or unit, a "SSI only" report will be submitted and the USACIDC element will offer assistance.

d. Hate bias graffiti investigations:

(1) Upon notification of incidents involving hate bias graffiti targeting specific individuals, USACIDC elements will initiate a preliminary investigation.

(2) Local USACIDC supervisors have the discretion to retain investigative purview on hate bias graffiti targeting specific individuals. If retained, the incident will be investigated and reported as a ROI/SSI. If the investigation is referred to the military police or unit, a "SSI only" report will be submitted and the USACIDC element will offer assistance.

(3) Hate bias graffiti located in public areas (e.g., walls in restrooms) and not targeting a specific individual will be documented in an appropriate file (i.e., Raw Data File). Local USACIDC supervisors have the discretion to retain investigative purview. If retained, the incident will be investigated and reported as a ROI/SSI, otherwise there is no reporting requirement.

(4) Hate bias graffiti found in open areas of the installation (e.g., rock in the middle of a field or a trash dumpster located next to the post exchange) and not targeting a specific individual will be documented in the appropriate file (i.e., Raw Data File). Local USACIDC supervisors have the discretion to retain investigative purview. If retained, the incident will be investigated and reported as a ROI/SSI, otherwise there is no reporting requirement.

e. Provoking speech/gestures with a hate bias motivation:

(1) USACIDC elements will not normally investigate incidents involving only hate bias speech or gestures. There are no reporting requirements for such incidents.

(2) Local USACIDC supervisors have the discretion to investigate these incidents. If investigated by USACIDC, it will be investigated and reported by a ROI/SSI.

f. USACIDC elements will record the proper NIBRS/DIBRS bias code(s) in the ACIRS III+ data base when identifying the offense(s) involved on all investigations determined to include a hate crime.

4-47
Sexual Assault Investigations

a. Definitions.

1. "Sexual Assault" is defined as those allegations involving the offenses of Rape, Indecent Acts or Liberties, Indecent Assault, Sodomy (forcible) and attempts and assaults to commit these offenses. It does not include Adult Private Consensual Sexual Misconduct (APCSM) offenses.

2. "Non-CID purview offenses" for the purposes of this paragraph are Conduct Unbecoming and Officer/NCO; Failure to Obey General/Lawful Order; Fraternization; Improper Relationship; Dereliction of Duty; Underage Drinking; Adultery; Adult Private Consensual Sexual Misconduct (APCSM) or other strictly unique military offenses. It does not include simple assaults, larcenies under $1,000.00 or other similar type crimes, which may be committed during the sexual assault

3. If, during the conduct of the sexual assault investigation, it is determined a non-CID purview offense(s) has been committed (such as described in paragraph 4-47a(2)) above, and does not include any aggravating circumstance, the matter will be referred in writing to the commander, without any further investigative action. The referral will be documented in the ROI.

4. If the allegation of a non-CID purview misconduct supports or contradicts the allegation of sexual assault, then the allegation of misconduct will be investigated only to the extent necessary to develop the primary offense of sexual assault. Under this circumstance, rights advisements will be administered when appropriate, but the misconduct offense will not be listed in the subject and/or victim blocks of the ROI, unless prior approval of the CG, USACIDC was obtained (See paragraphs 4-47c(6) and 4-47c(7) below). Non-CID purview offenses will be referred to the commander, in writing, for action deemed appropriate. The referral will be documented in the ROI.

5. If there are aggravating circumstances or the commander requests a CID investigation for the non-CID purview offenses, the CID unit will forward the matter, through its chain of command, to HQ, USACIDC for a decision prior to

the inclusion of the non-CID purview offense into any initial, status or final ROI, in accordance with paragraphs 4-47c(6) and 4-47c(7) below).

6. When seeking a CG, USACIDC decision whether t pursue a non-CID purview misconduct allegation because of aggravating circumstances or a commander's request, all available information will be forwarded through CID command channels to the HQ, USACIDC, Deputy Chief of Staff, G-3, Investigative Operations, ATTN: CIOP-OP. Electronic messages with chain of command concurrence/nonoccurrence are encouraged to expedite the process. The G-3 will review and forward the matter to the CG, USACIDC to determine whether to include the non-CID purview misconduct offense into the sexual assault ROI. No non-CID purview offense will be included in the ROI without prior approval of the CG, USACIDC. If immediate approval is required during other than normal duty hours, the information will be forwarded to the HQ, USACIDC Command Intelligence Operation Center (CIOC) or Staff Duty Officer (SDO) who will notify the G-3 of the request.

7. Any non-CID purview misconduct offense approved for investigation by the CG, USACIDC will include appropriate rights advisement to those involved, and the non-CID offense(s) will be listed in the subject and victim blocks of the ROI. Any non-CID purview offense(s) disapproved for investigation by the CG/DCO, USACIDC will be referred in writing to the appropriate action commander(s) and not further pursued in the ROI. The referral will be documented in the ROI.

8. The CG, USACIDC may delegate decision-making authority over non-CID purview misconduct allegation requests to the Deputy Commander, USACIDC.

4-48
Notification of Conflict of Interest Referrals

a. Definition: For the purposes of this policy, "Government employees" are formerly and current active duty soldiers, to include activated United States Army Reserve (USAR) and National Guard (NG), Department of Defense (DoD) and Department of the Army (DA) civilians.

b. Report of referral. When a ROI reporting a criminal conflict of interest offense (18 USC 203, 205, 207-209) committed by a current or former Government employee is referred for prosecution to a United States Attorney or the DOJ, the referring CID office will expeditiously notify (i.e., telephone, e-mail) the respective CID Group Judge Advocate. The Group Judge Advocate will, in coordination with the referring CID office, complete the OGE Form 202 and forward it to the Office of the Staff Judge Advocate, HQ, USACIDC, in a timely manner.

c. Interim Disposition. When there has been notice that the subject(s) of the referred conflict of interest ROI will not be prosecuted, the referring CID office will

expeditiously notify the CID Group Judge Advocate and provide all available information to include the date of the decision and any administrative, non-judicial or corrective action initiated or proposed.

d. Final Disposition. The referring CID office will notify the CID Group Judge Advocate of the final disposition of the subject(s) of the referred conflict of interest ROI and will forward a copy of the completed DA Form 4833 by the most expeditious means. The Group Judge Advocate will in turn forward the completed DA Form 4833 to the Office of the Staff Judge Advocate, HQ, USACIDC in a timely manner.

CHAPTER 5

5-1
Interviews

a. An interview of a military witness or potential witness does not normally require a warning of "rights." However, if, during the conduct of the interview, the special agent has any reason to suspect that a military person being questioned may have committed a crime, Article 31(b) of the UCMJ and Rule for Court-Martial 305(c) requires that the special agent must stop the questioning and advise the soldier of his "rights." Article 31(b) of the UCMJ and Rule for Court-Martial 305(c) requires that a soldier be read his rights when the soldier is suspected of having committed a crime, and the questioning is part of an official law enforcement investigation of disciplinary inquiry. It is presumed that questioning done by CID is for official law enforcement purposes. Both formal and Informal questioning in which an incriminating response either is sought or is a reasonable consequence thereof, is considered an "interrogation" which requires rights warnings.

b. Often, advising a soldier of his rights has a chilling effect on future conversations with the soldier. Nevertheless, even if a military witness is suspected of committing a minor criminal offense for which no disciplinary action is expected, he must still be advised of his rights. In the event such a soldier invokes and refuses to talk to the agent, and the testimony is considered essential, the agent should discuss obtaining a grant of testimonial immunity with the trial counsel.

c. Like an interview of a military witness, an interview of a civilian witness or potential witness does not normally require a warning of "rights." However, the 5th Amendment requires that warnings be given anytime an individual is "in custody at the station or otherwise deprived of his freedom of action in any significant way." Miranda warnings must be given when the person in custody is subjected to either express questioning or its functional equivalent, i.e., words or actions on the part of the police which the police know, or should know, are reasonably likely to elicit a response from the suspect.

d. The use of telephonic interviews to obtain or clarify information of minor significance is authorized and encouraged. Telephonic interviews can be useful in precluding a request for assistance when the person to be interviewed is in another unit's area of responsibility. Special agents and supervisors must consider the expected results before telephonic interviews are conducted to ensure that this type of interview is appropriate.

e. Requesting information from a person, firm, or government entity through use of letterhead stationary, may also be appropriate. Special agents and supervisors again must consider the expected results to ensure this approach is appropriate.

f. When conducting interviews, technical subject matter experts may be used to assist the special agent with technical issues or particularly complex subject matter. When used, the following should be observed:

(1) Discuss the case with the subject matter expert in advance to the extent necessary to ensure his understanding of the interview. Also, discuss the interview itself, so that the expert understands the role he is to play and exactly what the extent of his involvement will be.

(2) Consider not identifying the expert as such to the person being interviewed. This avoids creation of an atmosphere in which the interviewee feels he must compete to establish his own competence. Also, interviewees may be less willing to talk if they are aware that a listener can detect erroneous information.

(3) The technical expert should be thoroughly debriefed after the interview, with a written statement obtained in his own words. This ensures that a detailed record is available for future use and that technical terms and concepts are accurately recorded.

g. Business entities may request the presence of their legal counsel at interviews of employees who are or may be witnesses to criminal activity. There is no legal requirement that such counsel be present at witness interviews and the special agent must use his discretion as to whether counsel's presence may aid or hinder the interview and investigation. If such counsel is present, another government witness, preferably a government attorney, should also be present.

5-2
Interrogations

a. The 5th Amendment requires that warnings be given to a civilian anytime an individual is "in custody at the station or otherwise deprived of his freedom of action in any significant way." Miranda warnings must be given when the person in custody is subjected to either express questioning or its functional equivalent, i.e., words or actions on the part of the police which the police know, or should know, are reasonably likely to elicit a response from the suspect.

(1) Technically, USACIDC special agents can neither arrest nor apprehend civilians. They may, however, detain civilians on-post until such time as they can be surrendered to local, state, or federal law enforcement authorities off the installation. During this "detention" period, the civilian is not free to leave, hence any interrogation should be considered a "custodial interrogation" requiring a proper warning of rights. A USACIDC special agent must inform the civilian suspect/ subject that he has the right to remain silent, that anything he says can be used against him in a criminal trial, and that he has a right to talk privately with a lawyer before, during and after questioning. He should also be informed that if

he wants a lawyer but cannot afford one, then one will be appointed for him before any questioning begins. A civilian detained by USACIDC, who requests legal counsel during the rights advisement process, effectively shuts down all further questioning by special agents because the USACIDC cannot have counsel made available for the civilian suspect/subject. The request for counsel will be dealt with during the individual's initial appearance before a U.S. magistrate who will determine the need for appointed counsel.

(2) A civilian suspect/subject who freely wishes to be interviewed concerning a USACIDC investigation, and who was not detained in any manner, may be interviewed ("non-custodial"). A rights advisement is not necessary during a "non-custodial" interview. The civilian suspect/subject must clearly understand that he may freely terminate the interview at any time. If a joint investigation is being conducted with another law enforcement agency or the investigation may be referred to another law enforcement agency, prior coordination should be made with the interested law enforcement agency.

(3) Refer to paragraph 5-4f for further information concerning interrogation of employees of the federal government.

b. Prior to interrogating a military suspect/subject, a proper rights warning must be given. The USACIDC special agent must inform the suspect/subject soldier of the nature of the accusation, that he has a right to remain silent, and that any thing he says can be used against him in a trial by court-martial. In addition, according to Military Rules of Evidence, 305(d), if:

the soldier is in custody;

could reasonably believe himself to be in custody;

is otherwise deprived of his or her freedom of action in any significant way;

charges have been preferred against him, or;

the soldier has been or is still subject to pretrial restraint;

then he must also be informed that he has a right to have counsel present at the interrogation. If the soldier's company commander or supervisor directed the soldier to talk to the CID agent in a certain place, the soldier could argue that he was not free to leave the interview since his superior had ordered him there to talk to the CID agent.

5-3
Interrogation Procedures

The following procedures are generally applicable to both civilian and military suspects/subjects:

a. The rights warning will be accomplished utilizing a Rights Warning Procedure/Waiver Certificate (DA Form 3881). See figures 5-2 and 5-3.

b. Individuals will not be detained for interrogation unless an apprehension based upon probable cause has been made. Individuals not so detained will be advised they are not under apprehension or detention and that they may leave at any time.

c. Generally, after a suspect is read his Miranda rights with regard to a specific offense, he may voluntarily waive his rights and answer the questions of the CID agent. However, there is case law to suggest that even after being advised of his Miranda rights, the suspect/subject cannot make a valid waiver of his rights in certain situations. The decision chart at figure 5-1 will help the CID agent determine whether the suspect has made a valid, voluntary waiver of his rights. Before substantive questioning begins, the suspect/subject should be asked the following preliminary questions and the answers should be documented on a sworn statement form:

(1) Has the suspect/subject previously invoked his right to counsel with respect to this offense? If the answer is yes, proceed to question (2) below. If the answer is no, proceed to question (4) below.

(2) Has the suspect/subject been in continuous custody? When a suspect invokes his right to counsel while in a custodial interrogation, and he remains in continuous custody, then the police may not initiate a subsequent interview unless the suspect's attorney is physically present when the suspect is being questioned. If the answer is yes, the physical presence of the attorney is required before questioning can begin. If the answer is no, proceed to question (3) below.

(3) Has the suspect/subject seen an attorney? If the answer is yes, contact that attorney before going any further. If the answer is no, conduct the interview if the suspect/subject has had a "reasonable opportunity" to consult with counsel.

(4) Has the suspect/subject been questioned as a suspect regarding any other crime in the last five years? This question is meant to encompass crimes that are still within the statute of limitations, and which might require the agent to contact the suspect's/subject's attorney. If the answer is yes, proceed to question (5) below. If the answer is no, conduct the interview unless counsel has been appointed for or retained by the suspect/subject with respect to the offense in quest ion.

(5) Did the suspect/subject invoke his right to counsel with respect to the other alleged crime? If the answer is yes, proceed to question (6) below. If the answer is no, conduct the interview unless counsel has been appointed for or retained by the suspect with respect to the offense in question.

(6) Is the other crime still pending disposition? Once an investigator is on notice that an attorney has undertaken to represent an individual in a military criminal investigation, further questioning of the accused without affording counsel reasonable opportunity to be present renders any statement obtained involuntary. If the answer is yes, contact that attorney before going any further. If the answer is no, conduct the interview unless counsel has been appointed for or retained by the suspect/subject with respect to the offense in question.

(7) Regardless of the circumstances above, an accused can make a valid waiver of his rights if he initiates the conversation. Even when a suspect has previously invoked his rights on a particular offense, and he remains in continuous custody, he may waive his rights if he initiates the conversation. When a suspect/subject has retained a lawyer for advice relative to the matter under investigation, but subsequently approaches a special agent and indicates a desire to talk about the matter, the special agent will, in addition to the normal rights warning, if appropriate, obtain a waiver from the individual in which the individual clearly states that he is aware of the right to have the lawyer present during the interview and t hat contrary to the lawyer's advice he does not want the lawyer present. Details of the waiver will be included in the individual's statement, on the DA Form 3881, or in the narrative as appropriate.

(8) If a lawyer appears without prior knowledge of or request by the suspect/subject and wants to represent the suspect/subject, the special agent will inform the suspect/subject of his presence and offer the suspect/subject the opportunity to consult with the lawyer, or to decline to do so. There is no requirement that the lawyer be brought into contact with the suspect/subject in order to offer the opportunity for consultation. Any interviews/interrogations in progress need not be interrupted to advise the suspect/subject of the arrival of the unsolicited lawyer.

(9) If individuals do not wish to be questioned, they will not be questioned and their declinations will be reflected in the AIR narrative.

EXAMPLE

PV2 Vera Swift; 222-22-222; A Co, 43d Messkit Repair Bn, Ft Simpson, AL: At 1300, 1 Jul 94, SWIFT was advised of her rights by SA John DOE. SWIFT declined to waive her rights or say anything.

(10) If the individual does not want to consult with a lawyer and does want to answer questions, the person will be requested to complete a waiver on DA 3881. If the person declines to do so, the interrogation may continue and the fact of the verbal waiver and refusal to execute a signed waiver will be noted on the DA 3881 and in the AIR narrative, together with the names of any witnesses who are present.

EXAMPLE

PV2 Ima M. POSTER; 123-45-6789; A Co, 599th S&T Bn, Fort Simpson, AL: At 1300, 1 Jul 99, POSTER was advised of her rights by SA Aaron GROSS. POSTER declined to consult with a lawyer and agreed to answer questions, but refused to execute a written waiver. Her verbal waiver was witnessed by SA Karl O. SWENSON; Fort Simpson District, USACIDC.

(11) Whenever possible, a written statement will be taken from suspects and subjects utilizing DA Form 2823, Sworn Statement. The suspect/subjects own words will be used to the greatest extent possible, especially when using strange phrases and street language. However, in the statement, the agent should inquire as to the meaning of the language. If individuals elect to prepare their written statements on documents other than DA Form 2823, they will be allowed to do so. Special care will be taken to see that any written statement and/or notes will be secured in the file and retained for purposes of the Jencks Act. Special agents will then request the individuals to allow the affidavit appearing on the DA For m 2823 to be added and to execute the affidavit under oath. If the individual agrees, this will be accomplished. If the individual refuses, the documents will be accepted and explanatory remarks will be included in the AIR narrative.

EXAMPLE

PV2 Ima M. POSTER; 123-45-6789; A Co, 599th S&T Bn, Fort Simpson, AL: About 1300, 1 Jul 99, POSTER provided a written statement in which she confessed to stealing the trailer, however, she refused to swear to its truthfulness (Ex 27).

(12) Refer to paragraph 5-10d(2) concerning the use of video or audio taping.

5-4
Special Interviews/Interrogations

a. Senior personnel

(1) A senior person is a general or flag officer on active duty or retired; a member (or retired) of a Reserve Component or National Guard; a general officer designee (promotable 0-6); a DA civilian in the grade of GS-16 or higher; or other

person of equivalent rank who occupies a key position as designated by an appropriate commander.

(2) Whenever an allegation of criminality or impropriety against a senior person is received, the DCSOPS, USACIDC, will be notified immediately by telephone of the allegation(s). The telephonic notification will be followed up with a hard copy notification in the same format as specified in paragraph 5-4a(6) and (7) below. Unless otherwise specifically directed, this telephonic notification does not constitute authorization for the interview of the senior person as required by this regulation. A determination will be made at HQUSACIDC if it is a USACIDC responsibility or Department of the Army Inspector General (DAIG) responsibility to investigate the allegation. Follow-up reports will be in accordance with instructions provided by HQUSACIDC. Senior personnel will not be interviewed as a suspect/subject without specific prior authorization from HQUSACIDC, as specified in paragraph 5-4a(5).

(a) The preliminary inquiry conducted on allegations of criminality or impropriety against a senior person will be expeditiously pursued by the investigating element. A decision will be made within 7 business days that either the allegation is credible, resulting in the initiation of a ROI; that the allegation has proven to be unfounded, resulting in the closure of the preliminary inquiry; or that the credibility of the allegation cannot be determined, and an extension is necessary to complete the preliminary inquiry.

(b) By COB on the seventh day, the DCSOPS, USACIDC, ATTN: CIOP-ZA, will be notified of the results of the preliminary inquiry - ROI initiated, action closed, or request for extension submitted. A request for extension will include an investigative plan and time line for resolving the investigation. Notification will be done telephonically or by message providing that such notification is received NLT COB by the seventh day.

(c) Preliminary inquiries conducted on senior personnel that do not result in a ROI will be reported on a Criminal Intelligence Report (CIR) to DCSOPS, USACIDC, ATTN: CIOP-IN. The CIR will be submitted in hard copy on CID Form 97 and not by message. A copy of all related documents, statements, photographs, etc., will be attached as exhibits to the CIR. Distribution will be limited to the preparing office, the USACIDC major subordinate command, and HQUSACIDC. A complete copy of all exhibits will be included with the HQUSACIDC copy.

(d) When the inquiry not resulting in a ROI has been completed, the senior person concerned will be provided with an exit briefing on the findings of the inquiry. The exit briefing will include informing the senior person that the record of this inquiry and all related reports and documents will be forwarded to and stored at HQUSACIDC where it will be indexed and retrievable by name. The senior person will also be advised that release of this information will be limited to those

circumstances approved by the Commanding General, USACIDC. Individual concerns over the retention of such information and reports will be addressed to the Commanding General, USACIDC.

(e) The results of action taken against senior personnel resulting from any inquiry/investigation conducted by USACIDC must be closely monitored and reported to this headquarters in accordance with guidance provided by the DCSOPS, USACIDC, cited in paragraph (2) above. Such timely reporting is essential for this headquarters to comply with reporting requirements established by the DODIG and supported by the DAIG for all cases involving senior personnel.

(f) If the originating CID element feels that an "outside" investigating team from another CID element would be better suited to conduct the inquiry, this matter should be discussed with the appropriate field office/district or equivalent office commander and the USACIDC major subordinate command for resolution. In any event, the seven day limit on the preliminary inquiry will not be delayed pending the identification and transportation of the "outside" team to conduct the inquiry.

(3) When a senior person reports to either the military police or USACIDC field element that he/she is a victim of, or witness to a crime, the senior person will be interviewed to begin the investigative process. Subsequent to the receipt of such a complaint or report, and the interview of the senior person, the USACIDC field element will notify the DCSOPS, USACIDC of the purpose for, and results of such an interview. See paragraph (7).

(4) Whenever a senior person needs to be interviewed as a victim or witness to an investigation, the field element concerned will conduct the interview in accordance with normal investigative procedures. Upon completion of the interview, the field element concerned will notify the DCSOPS, USACIDC, of the results of the interview as required by paragraph (7).

(5) When a senior person initiates direct contact with a CID special agent or supervisor for the purpose of providing or reporting information, suspicions, allegations, or concerns of criminal misconduct, no prior authorization or approval is required from HQUSACIDC. After the interview, the DCSOPS, USACIDC, will be notified as specified in paragraph 5-4a(3), above, unless the senior person has been classified as a registered source in accordance with chapter 14.

(6) All requests for authorization to interview a senior person as a suspect/subject will be sent expeditiously to the DCSOPS, USACIDC, ATTN: CIOP-ZA. Express mail, electrical message, electronic mail, telecopier/FAX, or similar means may be used to accomplish this. When time is critical, notification may be made telephonically with written follow-up. After normal duty hours, notification to the DCSOPS will be made through the HQUSACIDC staff duty

officer (SDO). In all such actions, care must be taken to minimize exposure of sensitive information or potential public embarrassment of the senior person and/or the U.S. Army.

(7) An interview authorization request, or notification of interview, concerning any senior person(s) will be made to the DCSOPS, USACIDC, in the following format:

(a) Reporting/requesting CID unit

(b) Name of senior person(s) involved

(c) Grade and title of senior person(s)

(d) SSAN (if known) of senior person(s)

(e) Position of senior person(s)

(f) Offense(s) involved

(g) Relationship of senior person(s) to the investigation (e.g., subject, suspect, witness, victim, complainant, etc.)

(h) Name, grade, and unit or address of suspect/subject, if different from the senior person(s)

(i) CID ROI or sequence number

(j) When prior authorization is required, provide a brief summary of the facts, to include the issues sought to be resolved by the requested interview. A summary of the results of any senior person(s) interview conducted will be forwarded by electrical message, electronic mail, or FAX within one working day of completion of the interview.

(8) The distribution of reports involving senior person(s) will be as specified in chapter 8.

(9) No request for authorization to interview or notification of interview of a senior person is required or desired when a senior person is periodically briefed on current investigations and CID activities within his/her area of responsibility. This is considered to be a routine function and responsibility of CID supervisors and special agents which is done during the normal course of duty and is not an interview under the requirements set forth above.

b. Juvenile offenders

(1) The interview/interrogation of juvenile suspects is limited by applicable provisions of the Juvenile Justice and Delinquency Prevention Act of 1974 (18 USC 5031 et seq.). Whenever the custody, or implied custody of a juvenile is effected, the requirements and restrictions of the Juvenile Delinquency Act are involved. Most USACIDC investigative activities involving juveniles do not require taking the juveniles into custody.

(2) Juveniles will normally be interviewed in a non-custodial setting, in accordance with the criteria and procedures as follows:

(a) A juvenile suspect may be interviewed under the following circumstance: the offense occurred on a military installation or other facility or property subject to DoD control. The parent or guardian of the juvenile will be advised of the interrogation rights of the juvenile. The juvenile will be advised of his rights against self-incrimination with the consent of the parent or guardian. The juvenile and parents will be advised that they may terminate the interview at any time.

(b) It must be clearly demonstrated that the juvenile's cooperation is voluntary.

(c) The juvenile will not be fingerprinted or photographed without the written consent of the juvenile and the parent/guardian.

(3) When a juvenile suspect is identified, efforts will be made to effect a transfer of investigative responsibility to the appropriate federal, state, local, or foreign juvenile authorities. In some jurisdictions, this may require USACIDC special agents to appear in juvenile courts. Completion of the USACIDC investigation should be accomplished by use of a referred report. In those instances where the civilian authorities do not have, or decline to assume investigative responsibility, the determination whether additional USACIDC investigative activities are to be conducted will be resolved as in other cases involving civilian suspects.

(4) When a CID special agent detains or takes a juvenile into custody, the following actions will be taken:

(a) The agent will immediately advise the juvenile of his rights in language understandable to the juvenile, promptly notify the parent or guardian of the juvenile of such rights and the nature of the offense, and notify the local SJA of the juvenile's custody status.

(b) In the event that custody cannot be transferred to the civil authorities within a reasonable and brief period, the SJA will be requested to notify the appropriate U.S. attorney of the juvenile's custody status and to bring the juvenile before a United States Magistrate (see 18 USC 5033 and chapter 6, AR 27-40). Under these circumstances, special agents will not attempt to interrogate the

juvenile, although any remarks made by the juvenile may be recorded. Questions ma y be asked to clarify such remarks, but questions will not be used as a subterfuge to conduct a general interrogation.

(c) The juvenile will not be fingerprinted or photographed without the written permission of a federal judge responsible for juvenile cases regardless of consent by the juvenile or the parent/guardian.

c. Offenses against juveniles

(1) See AR 608-1 (Army Community Service Program) for information concerning the Army Child Advocacy Program (ACAP). This regulation requires that all allegations of serious child maltreatment (child abuse and neglect) be reported as quickly as possible to the provost marshal for appropriate law enforcement action.

(2) Law enforcement participation in the functioning of the ACAP should be provided by the provost marshal. A USACIDC unit may provide advice and assistance to ACAP personnel as needed to assist them in performing their functions.

(3) Appropriate USACIDC units will investigate all incidents in which the USACIDC has investigative responsibility that are reported directly to the USACIDC as well as those referred by the provost marshal or ACAP personnel.

(4) The USACIDC will investigate actual or alleged incidents of child abuse (i.e., physical abuse, sexual abuse, or neglect) which take place within an organizational setting/facility (e.g., child development center, quarters-based family child care home, youth activities center, medical treatment facility, gymnasium, etc.) or an Army sponsored/sanctioned activity (e.g., youth sport/recreation activities, field trips, etc.). This paragraph does not apply to incidents of child abuse occurring within the family unit.

(5) Any USACIDC unit conducting an investigation involving child sexual abuse will maintain close coordination with local child protective services personnel. In many instances, these professionals may be of invaluable assistance in conducting interviews of child victims of sexual abuse.

Consideration should also be given to utilization of the "anatomically correct" dolls during interviews if required under the circumstances. In all cases where such interviews are conducted with the assistance of child protective services professionals, the USACIDC continues to be the primary investigative agency controlling such interviews. Any USACIDC units conducting such investigations should always bear in mind that such incidents are extremely sensitive and the utmost care should be taken when conducting such interviews.

(6) Interviews of victims of child sexual assault are extremely sensitive and subject to considerable scrutiny. Additionally, after an interview in which the child implicates an adult in a sexual assault, there may be considerable pressure on the child to recant the earlier statement. Refer to paragraph 5-10d(2) to consider the use of video and/or audio equipment to record such interviews.

(7) Normally, there is no criminal offense when there is a reasonable use of force by a person responsible for the juvenile's welfare or supervision (e.g., parent, guardian or person so legally empowered). The determination of whether a criminal offense has occurred requires that the facts and circumstances of the alleged offense be applied to:

(a) The UCMJ when military personnel are the offenders.

(b) Local laws when personnel not subject to the UCMJ are the offenders.

(8) Coordination should be accomplished with the local SJA when questions exist as to status of persons involved in alleged offenses against juveniles or the reasonableness of the force used.

(9) There is no provision for USACIDC units to approve or sanction investigation by non-law enforcement agencies (e.g., school, scouting, juvenile councils) in lieu of USACIDC investigation of alleged criminal acts against juveniles.

d. Juvenile witnesses. Prior to transporting or having a juvenile witness transported to the CID office, MP station, or other law enforcement activity for interview, a parent or responsible guardian should be notified if possible. Prior parental/guardian notification is not necessary during interviews at crime scenes, during area canvasses, etc.

e. Females

(1) There are no special requirements relating to the interview/interrogation of females, except when conducting a polygraph examination as outlined in AR 195-6.

(2) When females are interviewed/interrogated under circumstances which might lend themselves to later allegations of impropriety against the special agent, a witness should be present if reasonably available.

f. Civilian employee union representation:

(1) The Civil Service Reform Act (CSRA), 5 USC 7114(a)(2)(b) provides that at any "examination" of a civilian federal employee who is employed in a recognized collective bargaining unit represented by a labor organization, the employee is

entitled at his request to be represented by a union representative if the employee reasonably believes that the examination may result in disciplinary action against him. Judicial and administrative interpretations of this provision have held t hat the employee's belief will be tested by objective criteria, rather than a subjective probe into the employee's mind. Consequently, for practical purposes, at USACIDC interviews, the employee is entitled to union representation upon request, even though the USACIDC special agent may consider the employee to be only a witness and not a subject.

(2) This right to union representation specifically applies to criminal investigations by the USACIDC, and is in addition to any other right of representation by counsel that may apply.

(3) There is no requirement that special agents advise civilian federal employees of their right to union representation.

(4) Under existing interpretations of the statute, the employee is entitled to wide latitude in consulting and seeking effective assistance from the union representative, if one is present. Consequently, if in the opinion of the special agent the interview/interrogation is proving unproductive, either because of disruptive behavior of the union representative, or because the union representative, acting as a spokesman, is answering the questions rather than the employee, special agents are limited to the following alternatives:

(a) The agent may inform the employee that the agent is only interested in hearing the employee's own account of the matter under investigation and the agent may give the employee the option of continuing the interview without union representation or further interruptions, or terminating the interview, in which case the employee's decision to terminate the interview will be noted and the case will continue to be investigated without the employee's input.

(b) The agent may terminate the interview and inform the employee that the case will continue to be investigated without the employee's input.

(c) The FBI may be contacted and asked to conduct the interview. The FBI is specifically exempted from the restrictions of the CSRA. No right to union representation exists at FBI interviews/interrogations.

g. Members of the Judge Advocate General's Trial Defense Service. If it is necessary during the course of a criminal investigation to interview or interrogate a member of the Trial Defense Service, arrangements will be made to do so at the USACIDC office or other facility away from the offices of the Trial Defense Service. This is not intended to preclude a conference at the offices of the Trial Defense Service if such is initiated by a member of that service during the preparation of a case for trial. See also paragraph 4-9b.

5-5
Victim/witness assistance

a. All Army law enforcement personnel, in the exercise of their law enforcement and investigative duties, shall treat victims and witnesses of crime with dignity, courtesy, and with respect to their privacy. Furthermore, Army law enforcement personnel will assist them in obtaining medical, financial, or social services, if needed or requested. The supporting SJA is responsible for the Army's Victim/Witness Assistance Program. Law enforcement personnel will cooperate and coordinate their assistance activities with the Victim/Witness Liaison (VWL) officer. Specific requirements, guidance and services available to victims and witnesses are described in AR 27-10, Military Justice. The following procedures will be followed within the USACIDC:

(1) At the earliest appropriate time, a DD Form 2701, Initial Information for Victims and Witnesses of Crime shall be provided to crime victims and witnesses, if not previously provided. The purpose of the form is to notify crime victims and witnesses of their statutory rights to receive the services described on the form and which are further explained in AR 27-10. The form is also used to provide the names and telephone numbers of the special agent/investigator to obtain the status of the investigation; VWL official located in the installation SJA’s office who can describe available assistance; legal official who can provide prosecution information; and the individual that can provide information concerning medical and other compensation services.

(2) All CID offices will maintain AR 27-10 for use by special agents and will ensure that all special agents review chapter 18 to become familiar with the requirements and guidance. Chapter 18 provides detailed instructions and definitions used in the program and its applicability. The following is a summary of key topics addressed in the regulation:

(a) Definition for victim and witness.

(b) Victim/Witness Liaison (VWL).

(c) Identification of victims and witnesses.

(d) Rights of crime victims.

(e) Victim services.

(f) Property return and restitution.

(g) Limitations of services provided to witnesses.

(h) Protection of victims and witnesses.

(i) Notification to employers and creditors.

(j) Requests for investigative reports/documents.

(k) Confinement facilities responsibilities.

(l) Reporting requirements and responsibilities.

(3) Special agents will expeditiously notify the victim/witness VWL officer when a subject is released or escapes from CID custody.

(4) An appointed special agent from each appropriate USACIDC office will be a member of the installation Victim and Witness Assistance Council to establish workable agreements and controls unique to the supported installation to ensure compliance with AR 27-10.

(5) In overseas commands, the Victim/Witness Assistance Program will apply subject to treaty or international agreement. If victim/witness assistance programs are in existence in the foreign jurisdiction, special agents shall cooperate with them if it is within their capabilities.

b. The following reporting procedures are required of all USACIDC field investigating elements:

(1) Beginning 1 Jul 95, the number of initial contacts made with victims/witnesses, meaning the number of DD Form 2701(s) or similar notifications to victims and/or witnesses will be reported to the Army installation provost marshal, who is responsible for reporting the aggregate total number conducted by law enforcement personnel. If a USACIDC investigative element is not located on a military installation, an agreement with the nearest or appropriate Army provost marshal will be made to collect the data.

(2) The number of notifications will be collected and reported to the office of the provost marshal in the manner agreed upon with the provost marshal.

(3) One recommended method for collecting the number of notifications is to record the number of notifications per case file on CID Form 66, in block 11, Other Action. As CID Form 66 is annotated/updated with the number of notifications, a copy can be placed in a file folder by month or entered onto a log and filed under file number 195-2e. This method will provide a centralized file to collect the number of notifications.

5-6
Written statements

a. Written sworn statements will be taken from all consenting suspects and subjects.

b. Written sworn statements will be obtained from all victims. Written sworn statements will also be taken from complainants as appropriated (i.e., a complainant having specific knowledge of the crime to support elements of proof would require a written sworn statement to be taken and a complainant having only third party knowledge that the crime occurred may not require the taking of a written statement).

c. Written sworn statements will be obtained from consenting witnesses under the circumstances listed below:

(1) When the person is an eyewitness to crime or otherwise has personal knowledge of incriminating information pertaining to a suspect.

(2) When the verbal account is improbable, inconsistent, or appears to involve exaggeration, prejudice or favoritism (e.g., the witness whose statement concerns a close friend or acknowledged enemy).

(3) When the individual is uncooperative, in fear, or may be coerced to change his statement or might spontaneously change his story because of professional or personal relationships.

(4) When the information provided is complex or confusing and disputes may arise over what was said or intended.

(5) When the witness provides significant information and it is likely he will leave the local area and not be readily available to testify in person. Sworn statements may be used in support of administrative or non-judicial (Article 15) action, in lieu of testimony at Article 32 hearings, and if stipulated to, introduced at trial.

d. The above guidance on obtaining statements must be reasonably applied. Situations may arise in which it would be unnecessary to obtain statements. Examples might include aggravated arson cases in which a large number of victims relate essentially the same information or when rights advisements are given as a precautionary measure in screening interviews and possible suspects can be immediately eliminated.

e. When preparing sworn statements, care must be taken to ensure they are usable for the purposes intended. If statements are prepared for the military police, they may be attached as exhibits to the ROI, but a statement should be

obtained when the individual is interviewed by a CID special agent to ensure the result is legible and complete. The special agent-in-charge may determine that additional statements need not be taken by special agents when statements taken by the military police are legible and complete in reporting all pertinent facts. To avoid allegations that information was changed in a statement, "white-out" correction fluid and strike-over correction paper will not be used on sworn statements. Errors will be corrected by drawing a single ink line through the material to be deleted, the use of slash marks (////) through the incorrect entry, or by typing the correct letter over the incorrect one. Continuation pages will be prepared in accordance with instructions printed on DA Form 2823. It should be noted that the affidavit which indicates the person has read the statements, etc., is a part of the statement; therefore, a sworn statement never ends on page one regardless of the length of the typewritten information provided. As a minimum, statements prepared on DA Forms 2823 always consist of at least two pages.

f. Sworn statements may be prepared using computer form fill-in type programs, which prepare statements as a suitable substitution for the actual DA Form 2823.

5-7
Verbal statements

a. Verbal statements will not be taken from suspects/subjects who are willing to make written statements.

b. The results of interviews and interrogations will be described in the AIR narrative. Special care will be taken to see that notes or recordings from the interview are secured in the file and retained for purposes o f the Jencks Act.

c. Whenever special agents utilize the AIR narrative to record the gist of interviews, the accounts of the interview will contain those elements normally expected in a written statement.

d. To further enhance the recording of interviews in the AIR narrative, the following principles of style and content will be observed:

(1) The content of the interview should be the special agent's paraphrasing of the significant information given by the interviewee, but must be easily understood. The past tense, third person, will be used.

(2) The exact words or expression of the interviewee will be used when significant, and indicated by quotation marks.

(3) Each interview will be recorded in one continuous paragraph unless otherwise required for clarity.

(4) Whenever two or more persons are interviewed during the same general time frame and provide essentially the same testimony, these interviews may be presented in one entry in the format of a single interview. If there are minor variances between multiple interviewees, these differences will be clearly stated.

(5) Narrative entries, describing results of interviews of persons who provide information relevant to the incident under investigation, will include the rank, grade or title, full name, SSAN, and the address of the person interviewed unless this information has been recorded in a previous entry. Other data felt to be pertinent may also be added.

5-8
Certificates

a. Certificates of loss or damage are not required but may be utilized and are encouraged when they provide the best or most convenient means for establishing the facts they contain. If a certificate of loss or damage is not obtained, the information on the loss or damage will be recorded in the AIR narrative.

b. Certificates of injury will be established from medical records. See paragraph 5-9. If a certificate of injury or a copy of the medical record is not available or obtained, the information on the injury will be recorded in the AIR narrative.

c. Death certificates will be obtained whenever possible for all death cases.

d. Other certificates, such as birth or marriage certificates, may be required to support certain types of investigations. A birth certificate will not normally be required solely for the purpose of establishing the age of a person. Coordination with the supporting SJA should determine if a certificate is required or if an alternate means or record will suffice.

5-9
Medical records/medical information

a. Army medical records are the property of the U.S. Government and are subject to the same controls and access restrictions as other U.S. Government documents. Access is forbidden to all but medical treatment/research personnel. Exceptions t o this rule are provided for by AR 195-2 and paragraph 10-11, AR 340-21-1. "Doctor-patient confidentiality" relationships do not exist in the Army setting, never the less, legal, moral and professional considerations dictate that confidentiality be protected to the maximum extent possible.

b. When copies of medical records or extracts of information from medical records are necessary to support the criminal investigation, the medical records must be requested in accordance with AR 40-66.

c. This policy is not intended to limit CID authority to seize Army records pursuant to investigative need. Any such seizure should be coordinated with the supporting SJA and should only be done when the agent has reason to believe the record (s) being sought may be destroyed or altered if normal channels are used.

d. All requests for medical records or medical information will be submitted to the patient administrator of the medical treatment facility (MTF) concerned. In the absence of the patient administrator, such requests will be submitted to the individual designated for this purpose by the MTF commander.

(1) DA Form 4254-R (Request for Private Medical Information) will be used to request medical records/information and will identify the information needed and the reason for the request.

(2) In cases of urgent need for medical information (rape, homicide, child abuse, etc.), a verbal request to the patient administrator is adequate. In such instances, the agent will provide a written request and sign the DA Form 4254-R, as soon as practical.

e. Original medical records will normally remain under the control of the medical records custodian. (1) The medical records custodian will provide the original record when required as "best evidence" to the judicial, non-judicial or administrative authority requiring it.

(1) In those circumstances where the original medical records themselves, as contrasted to the information contained therein, may be of evidentiary value to the investigation, the CID special agent is authorized to take custody of the records. An Evidence/Property Custody Document (DA Form 4137) will be provided to the medical records custodian as receipt.

5-10
Photography/photocopied evidence

a. General. Photography provides the capability of making visual records. When taken in a logical sequence, photographs add another source of record information about the investigation.

b. Crime scene photography. All CID field units will routinely utilize digital cameras to expose and record crime scene photographs. The agent assigned to the investigation and/or supervisor(s) are responsible for determining the type

and quantity of photographs that should be taken at the crime scene. The photographs should provide an adequate and accurate record of the crime scene. The use of video equipment or 35mm film will be used as needed and warranted to properly and thoroughly document the scene.

c. Photographic processing

(1) General: All CID field units will use the installation's VISC for photographic processing support, when available. Unit commanders should coordinate with their Visual Information Support officer for regular support and for priority handling when required. Priorities for photographic processing support must be reasonable. Routine support of 5 days processing time from receipt of the request by the VISC to return to CID of processed images with contact sheet, or a single set of prints, should be sufficient for most cases.

(2) Digital Photography:

(a) Images are initially stored on a Personal Computer Memory Card International Association (PCMCIA) memory card. An image may be previewed at the scene and retaken if warranted. Once the agent departs the scene, none of the images exposed may be deleted. Upon return from the crime scene, the images will be transferred from the memory card to the computer hard drive and onto a recordable compact disc. The PCMCIA memory cards will then be reused.

(b) When saved to the compact disc, the images will be numbered sequentially. If using equipment or software other than that provided by USACIDC, all image files must be converted to .jpg format before being written to the compact disk. Refer to the transfer software documentation for procedures to convert files to the .jpg format. The files stored on the compact disc will initially be saved to a primary directory identified by the year and case sequence number and the CID unit number (Primary Directory-970001.101). The primary directory will contain all image files for that case. The sub-directory, ATTACHED, will contain the image files of photographs included in the photographic packet.

EXAMPLE:

Primary Directory - 970001.101
DSC00001.JPG
DSC00002.JPG
DSC00003.JPG
DSC00004.JPG
DSC00005.JPG
DSC00006.JPG
DSC00007.JPG
Sub-directory - ATTACHED
DSC00002.JPG

DSC00003.JPG
DSC00005.JPG
DSC00007.JPG

(c) The CD will be labeled in “pen and ink” with the full ROI number (0001-97-CID001-12345-7F2).

A separate CD will be utilized for each case. The CD will be forwarded to the USACRC for retention when no longer required at the field element.

(3) Wet Photography: On installations where the supporting VISC can support wet photography, VISC will normally provide a contact print, or a set of prints, of film(s) submitted for processing. The case agent and team chief/direct supervisor will review the prints to determine which exposures are required as exhibits. Selected negatives/prints can then be returned to the VISC for making final prints. Contact prints will be retained in the CID case folder after completion of the investigation. All negatives will be forwarded to the USACRC for retention when no longer required at the field element. On installations where wet photography cannot be processed by the supporting VISC, each office is responsible for coordinating for this type of processing to ensure the capability is available when needed. The facility identified to process these photographs must be able to ensure the integrity and security of the processing to avoid compromise of the images.

d. Use of video/audio tapes

(1) When equipment is available, the use of color videotapes should always be considered when processing and recording a major crime scene. This is especially important at death or other scenes when potentially significant actions, such as the removal of a corpse, are taking place and the use of still photographs will not provide an adequate recording of the event.

(a) Videotapes of crime scenes, to include those with an audio track bearing verbal comments of special agents processing the scene will be secured the same as other documentary evidence such as rights waiver certificates, sworn statements, or photographic negatives. The tapes will be listed as not attached exhibits to the final report, retained in the CID office files, and will be disposed of by erasing and reusing when retention of the case file is no longer appropriate. Crime scene videotapes may be retained by the local CID office after destruction of the case file if coordination between the CID supervisor and the SJA or civilian prosecutor determines such long-term retention is appropriate.

(b) Videotapes of crime scenes which have an audio track bearing inadvertently recorded substantive verbal statements by a subject present on the scene will be handled and maintained as physical evidence in accordance with AR 195-5 until no longer needed as evidence and final disposition is approved by

the SJA or civilian prosecutor. After final disposition is approved, tapes may be erased and reused as appropriate.

(c) When video tapes are made of crime scenes or for documenting other evidential aspects of an investigation, a new, unused tape will be used. Tapes will not be edited in any manner after the initial recording. A new audio tape will also be used when making audio recordings that have evidential value.

(2) Audio/video taping of interviews and interrogations.

(a) In some circumstances, it may be advisable to video and/or audio tape an interview or interrogation. Prior to any recording, a written affirmative consent (Fig 5-X) must be obtained from the principal, and other parties present must have knowledge of the taping and have given written consent prior to the interview. The use of video and/or audio taping should be considered in circumstances in which the written statement would not adequately capture the content of the statement, and/or the voluntary written statement may be questioned. Except when circumstances clearly preclude notification, coordination will be made with the prosecutor prior to any recording.

(b) Interviews of the victims and witnesses of extremely violent crimes, to include sexual assault, should be strongly considered for videotaping with audio. The decision to videotape the interview should be made after an initial interview is conducted.

(c) The rights advisement of suspects and subjects will be included in the recording if a decision is made to video and/or audio tape the interview.

(d) Interviews of victims of child sexual assault should be recorded in their entirety. The guidance provided in paragraph 5-12e for photographing juveniles will be followed when recording interviews by audio/video means.

(e) The special agent conducting the interview will start the tape with an introduction. The introduction should include the case number, date, time and location of the interview. The special agent will introduce all the parties being taped and they must verbally affirm that they have consented to the taping.

(f) The oath or affirmation must be administered by the agent, when appropriate, at the conclusion of the interview in the same manner as if the statement was a written one.

(g) At the conclusion of the interview, the agent will make a statement as to the time and date the interview was completed.

(h) At the conclusion of the interview, the tape will be taken as evidence. As soon as possible, a copy of the original tape should be made. The copy will

be used to make any required transcripts and be available for review by authorized individuals. Once a copy has been made, the original should only be removed from the evidence room when needed for court and for final disposition. Once a tape is taken as evidence it will not be altered. Additional interviews will be placed on separate tapes.

(i) Videotapes will be handled as physical evidence in accordance with AR 195-5 until no longer needed as evidence and final disposition is approved by the SJA or civilian prosecutor. A written transcript of audio tapes, or video-tapes with an audio track, should be made for use as an attached exhibit to the final report. After final disposition, the tapes may be erased and reused, as appropriate.

(j) In unusual circumstances, a video and/or audio tape of an interview may be made for training purposes. A written release must be obtained from the principal and all other participants. No tape will be used for training until all legal proceedings have been completed.

(3) Surveillance videotapes

(a) Videotapes of surveillances, to include those having audio tracks, which bear no visible or audio evidence of criminal activity need not be retained as documentary or physical evidence and may be reused as appropriate. Due to the possibility that a tape of this type may be exculpatory, which would require its surrender to defense counsel, the significance of a surveillance tape should be discussed with the SJA or civilian prosecutor prior to destruction or reuse.

(b) Videotapes of surveillances which document evidence of criminal activity will be handled and maintained as physical evidence in accordance with AR 195-5 until no longer needed as evidence and final disposition is approved.

(c) Videotapes of surveillance conducted outside of the U.S. which contain non-consensual audio track recordings must be handled in accordance with AR 190-53 and AR 195-5. A surveillance tape recorded within the U.S. which contains a non- consensual audio track must also satisfy the requirements of 18 USC 2518(8)(a). The SJA or civilian prosecutor must be consulted prior to final disposition or reuse.

(d) Surveillance tapes described in (c) above, which are subject to the provisions of 18 USC 2518(8)(a) and/or AR 190-53, will be forwarded to the Crime Records Center for long term retention in accordance with the procedures outlined in paragraph (4)(d) below.

(4) Consensual and non-consensual interceptions

(a) Within the U.S.: Audio, video, and audio- video recordings made with authorization obtained under the provisions of AR 190-53 or 18 USC 2516, will be sealed, maintained, stored, and disposed of pursuant to one or more of the applicable provisions AR 190-53; 18 USC 1518(8)(a); and AR 195-5. At a minimum, unless otherwise ordered by a court, these recordings will be handled as physical evidence in accordance with AR 195-5.

(b) In foreign countries: Audio, video, and audio-video recordings made with authorization obtained under the provisions of AR 190-53 will be handled and maintained as physical evidence in accordance with AR 190-53 and AR 195-5.

(c) In any event, no recordings or related records of this type shall be destroyed or transferred to another storage facility without the concurrence of the SJA or civilian prosecutor and, as applicable, without issuance of a court order, (18 USC 2518(8)(a).

(d) If such action is approved by the SJA, civilian prosecutor, or court, the recordings and all related records of this type will be transferred to the Crime Records Center for long- term retention once they are no longer required at the local level. To meet the requirements of AR 195-5, final disposition authority will be obtained from the SJA or civilian prosecutor. If the interception was conducted in the U.S. under provisions of 18 USC 2516, the Crime Records Center will also be provided with all court orders pertinent to the recordings.

(5) An exception to the provisions of paragraph (3) is videotape recordings of hypnosis interviews. These recordings will be treated as evidence until no longer needed. They will then be erased.

(6) Videotaping equipment will not be used to record the activities of persons in areas where they have a reasonable expectation of privacy, except when taping is authorized by a search warrant.

(7) Photographic support may be requested from the supporting USACIL when the servicing Audio Visual Support Center cannot be time-sensitive for high priority investigations, or due to the sensitive nature of the photographed material in which knowledge of such material could jeopardize the conduct of the investigation.

e. Photocopied evidence. All documentary-type evidence should be photocopied, if possible, and the photocopies should be included in the investigative report. Examples of evidence that may be photocopied for the report include, but are not limited to, official Army forms of all types, e.g., leave and earning statements, passes, health records, travel vouchers, military revaluation reports, requests for identification cards, ration control cards, application forms, death and marriage certificates, excerpts from local regulation not available Army-wide (e.g., USFK, USAREUR, and local command regulations), and U.S.

currency. The authority and procedures described in 18 USC 474 and 504, and paragraph 11-5, AR 25-30, The Army Integrated Publishing and Printing Program, must be followed for the inclusion of photocopy exhibits of paper money, checks, bonds, other obligations, and securities of the U.S. and foreign governments, in USACIDC reports of investigation. Though the regulation does not specifically address law enforcement agencies, the intent is to follow the same practices for reproduction. The procedures are:

(1) Illustrations must be in black and white;

(2) Must be less than three-fourths, or more than one and one-half times the size of the genuine instrument.

5-11
Crime scene and evidence processing

a. Proper processing of crime scenes ensures the detection, description, collection, preservation and evaluation of physical evidence necessary for the identification and conviction of criminal offenders. In addition to the collection of physical evidence, response to a crime scene contributes to a depth of understanding about the area which cannot be obtained through any verbal description, however detailed, and may result in the locating of witnesses who would not be identified otherwise. If a crime scene exists, it will be responded to and the response must be prompt.

b. Under the provisions of AR 195-2, CID special agents have complete control of crime scenes and are responsible for either completely processing the scene or releasing control to another official (e.g., another CID special agent, FBI, MPI, postal inspector, etc.). Crime scenes will not be released until it is absolutely certain there is no further use of the scene.

c. The techniques, materials, and equipment used for the processing and collection of physical evidence are continually evolving. It is the responsibility of each CID special agent to maintain technical proficiency, knowledge of current methods, legal considerations, and laboratory examination requirements.

d. Child Pornography, Adult Pornography and Other Obscene Matter. Title 18 USC, Sections 2251-2260, Sexual Exploitation and other Abuse of Children and Title 18 USC, Section 1460-1470, Obscenity, make it a federal offense to possess, distribute, import or transport (including by mail, common carrier or the use of a computer) what is commonly referred to as child and adult pornography (hereafter referred to as “prohibited images”). Child pornography is broadly defined as a visual depiction of a person under the age of eighteen engaging in sexually explicit conduct as defined in Title 18, section 2256. For additional information and guidance concerning evidence processing of child pornography

and other obscene matter, both digital and hard copy, refer to paragraph 12-8, Chapter 12.

e. Latent prints. Fingerprint evidence is one of the most positive means for identification of individuals.

(1) Major case prints will be obtained from all personnel identified as possibly handling evidence when latent print examinations will be required or are contemplated. Particular care must be taken to ensure that major case prints are taken from deceased individual(s) in all CID death investigations.

(2) Care must be taken to obtain clear major case prints which record all areas of friction skin on fingers and palms. Supervisors or evidence custodians should review major case prints prior to submitting laboratory requests. The requirement for resubmissions will be minimized if two sets of major case prints are routinely obtained.

(3) Whenever fingerprint evidence may be used in an investigation, all personnel present at a crime scene must be identified so elimination prints may be obtained, if necessary.

(4) Whenever record prints are forwarded to the USACIL for comparison with latent print evidence, both finger and palm prints (i.e., major case prints) will be obtained.

f. Chemistry and serology. Collection and evaluation of this evidence requires painstaking effort and is critical for many types of crimes especially death and sexual assault cases.

(1) Clothing of suspects and victims must be obtained in such cases, carefully kept separated, with particular attention to avoiding the loss of trace evidence.

(2) Hair and fiber evidence must always be considered.

(3) Samples should be obtained and submitted for laboratory examination in suspected arson cases for a determination of the presence of accelerants. Submission of accelerants may require special logistical support as accelerants cannot be sent through postal channels.

g. Firearms. In cases involving the discharge of firearms, the weapon will be submitted for safety and functioning checks at the crime laboratory.

h. A crime scene sketch will be prepared when it may later assist the special agent in remembering what was observed at the crime scene; when it may aid CID supervisors, supported commanders, and SJAs in visualizing the scene of

the crime; or when it may be presented in court to assist the court in understanding the facts and correlation of other evidence in the case.

i. Crime scene photographs are useful in refreshing the agent's memory of the crime scene and for presentation in court to acquaint the court with the appearance of the crime scene. Photographs also provide a permanent record of perishable or fragile evidence. The decision to take photographs should be based upon evaluation of the crime scene and the nature of the investigation. A prime factor to be considered is that if photographs are not taken during the crime scene processing, then such photographic evidence is lost and cannot be reconstructed. When exposed, photographs should depict all significant aspects of the scene, evidence, or elements of proof. Photographs will, as a minimum, be exposed to depict the following:

(1) All deceased subjects or victims.

(2) Injuries suffered by victims who have sustained extensive or grievous bodily harm.

(3) Crime scenes of all death investigations.

(4) Crime scenes where extensive damage or destruction of property have been committed.

(5) Crime scenes containing numerous items of evidence, especially when interrelationships and locations are important.

(6) Autopsies. Photographs should include identifying views of the body and specific coverage of features identified as significant by the pathologist or observed by the investigator. A measurement scale should be included in close-up photographs depicting wounds, marks and other features having evidential value. Videotaping of autopsies should be done only when necessary to record information or depictions of specific evidentiary value and when the use of still photographs will not suffice. The procedure will be coordinated with the pathologist prior to the autopsy. Autopsies will not be videotaped for training purposes.

(7) See paragraph 5-10d for policy on use of videotape at crime scenes.

j. Color film. Color film is preferred over black and white film in most aspects of investigative photography. The use of color film should always be considered for the following:

(1) Body photographs. Bruises, discoloration, marks, injuries, blood stains, are best depicted by the use of color photographs. Color photographs are required for autopsies and cases involving child abuse.

(2) Fire in progress, as a supplemental aid in identifying the flammables involved in the fire.

(3) Offenses meeting the Violent Criminal Apprehension Program (VICAP) criteria. See appendix F.

(4) Any situation in which evidence or matters of significance would be obscured or less clear if black and white film were used.

k. The decision to expose photographs or to attach photographs to the ROI must be based on a reasoned analysis of what they depict and whether they would contribute to the utility of the report to commanders, SJAs, etc. Photographs are not al ways required. Attaching a photograph which depicts nothing more than an empty parking slot where a stolen vehicle used to be parked usually contributes nothing to the case.

l. All special agents must be proficient in photography. Agents conducting investigations must be capable of exposing good photographs and supervisors must be able to recognize when guidance and training is required. Proficiency should extend not only to use of automatic functions but also specialized techniques such as close-up photography and off camera flash.

m. Unless dictated otherwise by the given situation/investigation, photographic exhibits will normally be either 4” x 6” or 5" x 7" size prints. Larger prints may be obtained as required for clarity. Photographs/prints will be attached to the ROI in the following manner:

(1) Photographs/prints will be marked with the appropriate ROI number and numbered sequentially on the front margin or other front area of the photograph which does not obstruct the photograph. The ROI number will be placed on a white background before being affixed to the photograph. Computerized labels trimmed to proper size work well to simplify this process.

(2) For digital photography images, part of the description will be the image file name. A photograph index page will be prepared on bond paper in the following format:

PHOTOGRAPHIC PACKET

CASE NUMBER

NUMBER	DESCRIPTION OF PHOTOGRAPH
_____	_____
_____	_____

_____ _____
_____ _____
_____ _____
_____ _____
_____ _____
_____ _____

EXHIBIT ___

FOR OFFICIAL USE ONLY

(3) The marked photographs/prints will be assembled into a photographic packet. If there are more than 20 prints, they will be separated into sub-packets, each sub-packet will not exceed 20 prints. An index page will be securely fastened to the front of the packet/sub-packet. Each packet/sub-packet will contain only the photographs/prints associated with the index page pertaining to the packet. When there are more than 20 prints and they are placed in sub-packets, the prints will be numbered consecutively so there are no duplicate numbers. Photographs/prints that are printed as full sheets (8”x10”) will be fastened together with the index page on top. When the prints are printed on smaller sheets (4” x 6” or 5” x 7”) they will be placed in a 8.5" x 11" (approximate size) envelope. The photograph index may be printed on the envelope if the capability exists. Alternately, smaller prints may be placed in a clear plastic 8.5" x 11" (approximate size) pouch with a single index page inserted in the front of the pouch. The photographic packet will be listed as a separate numbered exhibit of the report. The negatives or original images will be listed as a separate exhibit. If sub-packets are used, the report will reflect the number of sub-packets in the following manner with the sub-packets marked accordingly:

EXAMPLE

EXHIBITS:

Attached:

1. Statement of SSG Doyle, 5 Jul 94.

2. Rights waiver certificate and statement of SSG Constable, 5 Jul 94.

3. Medical examination report by MAJ Lee concerning SSG Doyle's injuries, 4 Jul 94.

4. Photographic packet comprised of 52 photographs.

a. Packet containing photographs 1-20.

b. Packet containing photographs 21-37.

c. Packet containing photographs 38-52.

5. Compact disc 970001.101 containing all photographic images and the originals of exhibit 4 (USACRC copy only).

6. Photographic packet comprised of 17 photographs (photographs 53-69).

7. Photographic negatives of exhibit 6 (USACRC copy only).

Not Attached:

None.

The originals of exhibits 1 and 2, and exhibits 5 and 7 are retained in the files of this office. The original of exhibit 3 is retained at the Walter Reed Army Medical Center.

Care should be exercised when attaching envelopes or plastic pouches to a ROI to prevent the loss of photographs/prints. Envelopes and pouches should be the variety that opens from the top with either a string wraparound, metal fasteners, or other securing feature.

(4) All negatives exposed during the investigation will be placed in an envelope. The envelope will then be stapled to plain bond paper, and listed as a separate numbered exhibit.

(5) Photographic negatives and the compact disc containing the original images should be retained by the investigating office until all legal proceedings are completed to ensure that additional photographs/prints are not needed for court or other proceedings. After all proceedings are completed, the photographic negatives and compact disc ROM will be forwarded to the USACRC.

(6) Photographic negatives may be receipted to the supporting SJA or prosecutor if additional copies or sizes of photographic exhibits are required for any legal proceeding. An original compact disc containing images will not be released. A copy of the disc will be made and released.

(7) Photographic negatives or contact prints forwarded to the USACRC will be marked to reflect which photographs/prints were used as exhibits of a ROI. All photographic negatives, whether or not included as an exhibit, are subject to

Freedom of Information Act and Privacy Act releases if they are part of the information on file at the USACRC.

(8) The compact disc will have a directory and sub-directory to clearly indicate which images were used as exhibits. (See paragraph 5-10c(2)(b))

5-12
Photographing persons

a. Photographs are taken of persons to:

(1) Aid in establishing the identity of the person.

(2) Aid in relating the person to the crime.

(3) Depict evidence of trauma (e.g., bruises, wounds). Note: Since many injuries do not achieve full coloration for some time, injury photographs should be taken immediately and should be retaken at sufficient intervals to show the progress of the injury.

b. Military suspects and subjects may be photographed without their consent. Reasonable force may be used, if necessary.

c. Military or civilian victims may be photographed provided they do not object. There is no requirement to inform them of their right to refuse. Victims should be photographed in ways which provide the greatest level of dignity. The victim should only remove the minimum amount of clothing and should be allowed to cover all non- injured areas of the body. If clothing is required to be removed to permit photography of an injury, such photographs should be taken by members of the same gender as the victim, or by a health professional, whenever possible. At a minimum, a member of the same gender should be present.

d. Civilian suspects and subjects may be photographed when they do not object. There is no requirement to inform them of their right to refuse. If there is an objection and the photograph is still desired, it should be obtained from the appropriate civilian authorities.

e. Juvenile subjects, suspects, or victims will only be photographed with the expressed consent of the juvenile and the parent or guardian. When in custody, a juvenile will not be photographed without the written consent of a U.S. magistrate, federal judge or other judge responsible for the case regardless of consent by the juvenile and parent or guardian. When the parent of the juvenile is the suspect/subject of an offense against the juvenile, the juvenile may be photographed provided the juvenile does not object. The fact that the juvenile is

incapable of objecting does not constitute a bar to the taking of photographs of the juvenile.

f. Covert photographs taken of suspects, to include juveniles, in a place open to public view incident to a covert surveillance may be obtained without consent. Covert photographs of suspects within their home or place where a person has a reasonable expectation of privacy constitutes a search and must be authorized by a search warrant. Covert photographs can, under certain circumstances, be taken of people in their homes under circumstances where the suspects will not be said to have reasonable expectation of privacy, e.g., in front of a plate glass picture window.

5-13
Fingerprinting persons

a. Fingerprints are obtained to:

(1) Aid in establishing the identity of the person.

(2) Aid in relating a person to a crime.

(3) Aid in relating a person to the crime scene or a specific piece of evidence.

b. Record and major case prints will be taken from all persons listed as suspects/subjects in a CID investigation. These fingerprints will be taken at the earliest opportunity normally during the initial interview and processing of the individual, except as noted below. Two FD-249s will be completed exclusively for file and disposition purposes. One DoJ R-84 will also be completed. Additional record and major case prints will be obtained to support all laboratory examinations required during the investigation. Exceptions are:

(1) Juveniles

(2) Civilian offenders who do not consent and the civilian authorities cannot or refuse to obtain them.

(3) Anyone listed as a subject in a Referred or Collateral ROI.

(4) In those instances considered by the CID supervisor to be inappropriate.

(5) An investigation will not be held in an open status merely to obtain fingerprints.

c. Military suspects/subjects may be fingerprinted without their consent. Reasonable force may be used, if necessary. Furthermore, the soldier's commander can order the soldier to submit to fingerprinting.

d. Military and civilian victims may be fingerprinted provided they do not object. There is no requirement to inform them of their right to refuse.

e. Civilian suspects/subjects may be fingerprinted when they do not object. There is no requirement to advise them of their right to refuse. If there is an objection and the fingerprints are still required, they should be obtained by the appropriate civilian law enforcement authorities.

f. Juveniles will be fingerprinted only with the expressed consent of the juvenile and the parent or guardian. When in custody, the juvenile will be fingerprinted only with the written consent of a U.S. Magistrate, federal judge or other judge responsible for juvenile cases, regardless of the consent of the juvenile and parent. When the parent is the suspect/subject of an offense against the juvenile, the juvenile may be fingerprinted provided the juvenile does not object. The fact that the juvenile may be incapable of objecting does not constitute a bar to fingerprinting the juvenile.

5-14
Submission of fingerprint cards (FD-249/R-84) to the FBI

a. For each military subject, one set of fingerprints on the FD-249 that meet submission requirement to the FBI in accordance with Appendix O, CIDR 195-1, will be submitted to the USACRC. Upon receipt of fingerprint cards from CID field elements, the USACRC will process the fingerprint cards utilizing the Automated Fingerprint Identification System (AFIS). Once processed, the fingerprint images will be forwarded for investigative and archive purposes with the FBI. Submission of the fingerprint cards to USACRC and subsequent processing and submission to the FBI by USACRC will be completed when the following command action occurs:

(1) If final disposition of the proceedings is anticipated within 60 days of command initiation of military judicial proceedings, or of command action in non-judicial proceedings (Article 15 by a field grade commander), except a summarized Article 15, the FD-249 may be held for the final disposition to be recorded.

Final disposition of judicial proceedings are defined as final approval of a resignation, retirement, or discharge in lieu of court-martial or when the trial counsel forwards the record of trial to the convening authority. If the final disposition of the proceedings will be after 60 days, then submit the FD-249 within 15 days of command initiation of military judicial proceedings (the referral

of court-martial charges to a court-martial, i.e., summary, special, or general court-martial by the convening authority) or for non-judicial proceedings as described above. If the final disposition is not recorded on the FD-249, then a R-84 is required after final disposition of the proceedings.

(2) Within 15 days after final disposition of judicial or non-judicial proceedings, or the approval of a request for discharge, retirement, or resignation in lieu of court-martial, disposition information shall be reported on the R-84 if it has not been reported on a FD-249. Dispositions that are exculpatory in nature (e.g., dismissal of charges, acquittal, act.) shall also be reported. Note: “Discharge in lieu of court-martial” refers to Chapter 10, Army Regulation (AR) 635-200, Enlisted Separations, and Chapter 3, AR 600-8-24, Officer Transfers and Discharges. Enlisted personnel may submit a request to the general court-martial convening authority (GCMCA) for a discharge instead of continuing with a court-martial. The GCMCA determines the characterization of service for the enlisted soldier. Officers submit a resignation in lieu of court-martial to the GCMCA who forwards it with recommendations to the commander, Total Army Personnel Command (TAPC). Final approval for officer resignations is the Secretary of the Army or their designee.

(3) Submission of fingerprint cards should normally take place in conjunction with forwarding of the final ROI if disposition is known and listed in the status section of the report, or at the time of submission of the DA Form 4833 (Commander's Report of Disciplinary or Administrative Action) to USACRC.

b. If applicable, a finding of lack of mental competence to stand trial shall be recorded as “final disposition” either on the FD-249 or R-84, as appropriate.

c. The submission of fingerprints through the USACRC to the FBI is required if the charges on the court-martial sheets or the Article 15 reflect an offense listed in appendix O, CIDR 195-1, even if they are different from those listed in the CID ROI. However, if the charges on the court-martial sheet or the Article 15 do not contain an offense listed in appendix O, CIDR 195-1, the fingerprint card will not be sent to the USACRC. Do not hold the FD-249 pending appellate actions; however, appellate action affecting the character of an initial disposition must be reported if it occurs. Dispositions that are exculpatory in nature (e.g., dismissal of charges, acquittal) shall also be filed. In those situations where an individual is acquitted on charges for offenses listed in appendix O, CIDR 195-1, but is convicted of offenses not listed in appendix O, CIDR 195-1, the acquittal, and offense(s) for which convicted, will be reflected on the FD-249 or R-84. Upon review and approval by the convening authority, final disposition will be recorded on the FD-249 or R-84, as appropriate, and forwarded to the USACRC within 15 working days of the date the review and approval was accomplished.

d. The charge(s)/offense(s) annotated on the FD-249 and R-84 will be expressed in literal terms (e.g., murder, rape, robbery, etc.) and not as a UCMJ

article. The charges annotated on the FD-249 must reflect the actual charges pursued through court-martial or non-judicial punishment even if different from those for which the individual was listed in the CID ROI. The disposition reflected on the FD-249 or the R-84 will be described in common language (e.g., dishonorable discharge, reduction in rank, forfeiture of pay, charges dismissed, etc.). The ORI number to annotate on fingerprint cards or related documents is "VAUSA1400."

e. The submission of the FD-249 will not be delayed pending completion of court-martial action. If the disposition of the court-martial is not known at the time the FD-249 is submitted, then the submission of the R-84 will be necessary.

f. The FBI DoJ R-84 will be submitted through the USACRC to the FBI to report the results or disposition of any judicial action taken against any individual whose fingerprints have already been transmitted to the FBI on the FD-249. The R-84 is not required if the disposition action was reflected on the FD-249 at the time of submission. The fingerprint submission chart at appendix O, CIDR 195-1 (figure O-1) should be referred to and used as a quick reference/guide and management tool to ensure timely submission.

g. One set of fingerprints on the FD-249 will be maintained in the case file for each individual whose fingerprints have been submitted to the USACRC.

h. Those fingerprint cards (FD-249/R-84) completed on individuals during the processing of the investigation, but not required for submission to the USACRC/FBI, will be retained in the case file. Only those fingerprint cards intended for submission to the FBI will be forwarded to USACR C.

i. Unless there is a specific need in an individual case, copies of the FD-249 and R-84 will not normally be included as exhibits to the ROI.

j. A specific entry in the Agent Activity Summary (CID Form 28) will be made to reflect the date(s) the FD-249 and/or the R-84 were submitted to the USACRC. Each investigation must be monitored to ensure a timely submission. An effective suspense system to facilitate monitorship should be implemented.

k. For each civilian subject: There is no requirement for CID to take or forward fingerprint cards or AFIS scan results of civilian subjects to the FBI. Normally, fingerprints of civilian subjects are taken and submitted to the FBI by civilian law enforcement authorities when the subject is processed through the criminal justice system. However, in the event CID has assumed exclusive investigative responsibility, fingerprint cards obtained of civilian subjects will be forwarded to the USACRC for submission to the FBI under the following conditions:

(1) When no other law enforcement agency has done so;

(2) When the offense(s) is comparable to those listed in appendix O, this regulation;

(3) Upon either an arrest or indictment for an offense comparable to those listed in appendix O, this regulation;

(4) When adjudication is under the United States legal system

l. For each juvenile subject: There is no requirement for CID to take or forward fingerprint cards or AFIS scan results of juvenile subjects to the FBI. Normally, fingerprints of juvenile subjects are taken and submitted to the FBI by civilian law enforcement authorities when the subject is processed through the criminal justice system. However, in the event CID has assumed exclusive investigative responsibility, fingerprint cards of juvenile subjects, obtained IAW CIDR 195-1, Chapter 5, paragraph 5-13(f), will be forwarded to the USACRC for submission to the FBI under the following conditions:

(1) When no other law enforcement agency has done so;

(2) When the offense(s) is comparable to those listed in appendix O, this regulation;

(3) Upon either an arrest or indictment for an offense comparable to those listed in appendix O, this regulation;

(4) When adjudication is under the United States legal system

(5) When the release is not in violation of 18 USC S5038 (Use of Juvenile Records). Coordinate with the supporting trial counsel to ensure submission meets the requirements of 18 USC S5038.

5-15
Identification photographs files (mug files)

a. Each USACIDC unit, except branch offices and EC fraud units, will maintain an identification photograph file (mug shot) unless exempted by the appropriate USACIDC major subordinate command. The file will consist of photographs of adult suspects/subjects identified as a result of criminal investigation activities conducted by the unit or other law enforcement agencies. The file should consist of photographs of suspects/subjects involved in the types of crimes where experience indicates that photographs may be of value in possible future identification. Photographs included in the file may be those obtained:

(1) In accordance with paragraph 5-12.

(2) From any other source (e.g., administrative files, other police agencies) when there is credible information that the person portrayed has been, is, or may become, the perpetrator of a DoD related crime of interest to the USACIDC unit.

b. Identification photographs may be taken using a 35mm camera, digital camera, or a Polaroid camera. Identification photographs may be taken with either color or black and white film. The photographs must be standard in size and appearance (color vs. black and white). If the identification photographs are for a request for assistance from another office, the requesting office format standard must be followed. The photograph should be a full-face view of the individual from mid-chest to top of the head. Profile, oblique, or rear photographs may be taken, when deemed appropriate. Marks such as scars, tattoos, and blemishes, which are not clear in the full-face picture, may be photographed and indexed (See paragraph 5-15d).

c. No personal identification markings or codes will be shown on the face of the photograph. If such markings are on the photograph, they should be covered or blacked out. The subject should wear an unmarked over- blouse or jacket to cover unit patches, nametags, rank, etc. If paper photographs are used, the reverse side of the photograph will either have identifying data concerning the person depicted or some index system that identifies the person depicted. The photographs may be arranged by sex, ethnic background, physical characteristics, or other distinctive grouping. The file should protect the photographs from loss and provide for the ready removal and addition of photographs as needed.

d. The identification file will be indexed. This index may consist of CID Form 44s, DA Form 2804s, a ledger book, an automated database or some other suitable, locally determined, manner. The index will provide an easy procedure for identifying photographs and determining the correct position of the photograph in the file. The index may be annotated with physical or unusual characteristics of the person not visible in the photograph and other information, such as ETS and DEROS to assist in purging the file. The file should include the index number of the photograph to assist in locating a photograph when only a name is known.

e. In the event a subject from a previous ROI is identified as a subject of a subsequent ROI, the original photograph may be carried forward, if it is still a valid likeness, or a new photograph may be made. If a new photograph is used, the old photograph should be retained for possible future use.

f. It is appropriate to allow a potential witness to view a particular distinctive grouping of the identification photograph file when the special agent does not suspect a particular person of being the perpetrator.

g. A line-up is appropriate when a particular person is suspected of being the perpetrator. The photographs used in a photographic line-up must have a uniform appearance in order to prevent possible judicial claims of irregularity in photograph identification procedures. Anything that could make a subject's photograph differ unreasonably from others in the line-up must be avoided (e.g., the subject's photograph is larger than the others).

5-16
Line-ups

a. A line-up is appropriate when:

(1) A witness may be able to recognize a perpetrator of a crime.

(2) The witness does not know the identity of the perpetrator, but the special agent suspects one or more persons of being the perpetrator.

b. Line-ups may be either physical or photographic. A physical line-up is preferred to a photographic line-up unless:

(1) The presentation of a physical line-up would unduly delay the investigation.

(2) The witness is fearful of confronting a physical line-up and facilities are not available which will preclude a confrontation.

c. Physical line-up. Special agents should be aware that there are differences in the conduct of line-ups depending on whether a suspect or subject is included in the line-up.

(1) A physical line-up must be conducted in all its aspects so that it is essentially fair. There must be no suggestion as to which participant the special agent suspects of being the perpetrator.

(a) There should be six or more participants wherever possible.

(b) The participants should be reasonably similar in appearance (i.e., sex, race, age, height, weight, hair, glasses, clothing).

(c) There should be three or more viewings with the positions of the participants varied each time.

(d) Each viewing will be photographed and the photographs retained in the case file for future reference. Participants will be identified by the use of position numbers or letter cards displayed for each participant.

(2) Prior to a physical line-up, each suspect will be informed:

(a) Of the purpose of the line-up.

(b) Of the general procedures to be followed during the line-up.

(c) That a military subject who has been apprehended based on probable cause may not refuse to participate in the line-up. A military suspect who has not been placed under apprehension and civilians may not be forced to participate in a military line-up.

(d) When the line-up is conducted with a subject in a custodial situation, such as pretrial, military police custody or pending pretrial, he will be afforded the right to consult with an attorney. The subject may waive the rights provided in MRE 321, MCM, if the waiver is freely, knowingly, and intelligently made.

(3) Suspects/subjects do not have the right to refuse to provide speech exemplars.

(4) If a suspect/subject requests the presence of a lawyer, the lawyer will be allowed to observe the line-up and to make recommendations, but will not be allowed to control the line-up or witness(es).

(5) Only one witness at a time should view the line-up.

(6) The conduct and the results of the line-up will be documented in the narrative of the ROI.

(7) Suggested procedures for conducting line-ups are provided in FM 19-20.

d. Photographic line-ups

(1) A photographic line-up, like a physical line-up, must avoid suggesting to the witness who the special agent suspects of being the perpetrator.

(a) There will be six or more photographs used to conduct the line-up.

(b) The persons portrayed in the photographs should be reasonably similar in appearance.

(c) There should be three or more viewings with the positions of the photographs varied each time.

(2) There is no requirement for the suspect/ subject to be informed or be present at a photographic line-up, nor is there any requirement that a lawyer observe the conduct of the photographic line-up.

(3) The special agent conducting the photographic line-up will identify in the ROI narrative which photographs were used, their positions in the line-up, and the results. Photographs should be taken of each layout of the photographic line-up for future reference.

5-17
CID wanted poster

a. General. CID Wanted Poster (CID Form 88) may be used when:

(1) A representation of facial characteristics is available or can be fabricated (i.e., a photograph or identikit composite), but identity is unknown.

(2) A facial representation is available and identity is known, but the wanted person cannot be located.

b. Prerequisites

(1) Because of the potential damage to the reputation of the person portrayed in a wanted poster, a CID Form 88 will be prepared reflecting that a person is wanted as the perpetrator of a crime only when the special agent has some credible information that the individual may have committed the crime, and that the crime is within the investigative responsibility of the USACIDC. (See figure 5-6).

(2) If a reward is announced on a wanted poster, the following notice will be included in the reward statement: "This reward will terminate on (enter date one year from the date the reward was authorized)." See AR 195-4 for further guidance concerning rewards.

c. Distribution. CID wanted posters may be distributed:

(1) Within DoD to include posting at any place on the military reservation. However, appropriate coordination should be accomplished in advance with the installation.

(2) To appropriate non-DoD law enforcement agencies.

d. The use of a wanted poster will be documented in the AAS.

e. The complete ROI number (less offense codes) will be included on the wanted poster.

5-18
Controlled substances

a. Although some responsibility for investigating certain controlled substance offenses has been delegated to the military police, the USACIDC is charged by AR 195-2 with overall responsibility for investigative activity involving controlled substances.

b. Special provisions relating to the investigation of offenses involving controlled substances are found in chapter 13.

c. Shared possession/use of a controlled substance involves two or more people sharing an illegal drug during communal personal consumption. The act of sharing an illegal drug during consumption is Wrongful Distribution of a Controlled Substance under Article 112a, UCMJ. However, CID elements will not list or title any subject(s) for distribution of an illegal substance based solely on the act of sharing the drug during communal consumption. In such cases, the cited offense(s) will be Wrongful Possession and/or Use of a Controlled Substance. The CID decision not to cite Wrongful Distribution of a Controlled Substance in such incidents does not preclude a commander or SJA from using that offense in any subsequent administrative or judicial proceedings.

5-19
Bomb threats

a. The USACIDC response to bomb threats will be to monitor the military police response and to assist/respond as appropriate. Response/assistance is required when requested by a provost marshal, unit commander, installation commander or as determined necessary by a CID supervisor. Pertinent military police documentation concerning the incident will be obtained for review and determination of the level of USACIDC involvement.

b. A criminal investigation will be initiated on bomb threat incidents when a bomb is located or detonated, a subject is identified, or a series of related threats occur. In all other bomb threat incidents, a detailed AAS will be prepared and the sequence number action completed.

c. Bomb threats pertaining to off-post locations will be referred to the appropriate civilian law enforcement authority.

5-20
Hostage situations

a. The installation commander is the individual responsible for controlling hostage situations to include the restoration of order, the safety of the hostages, and all negotiations, in accordance with AR 190-52.

b. The installation commander may task USACIDC personnel to assist in hostage situations. The individuals so tasked will temporarily be placed under the operational control of the installation commander who will direct their activities and be responsible for their actions. These USACIDC personnel will respond to the directives of the installation commander and will act in the commander's behalf.

5-21
Death investigations

a. Definitions of Terms:

(1) Manner of death is the legal classification of death, whether it be natural, suicide, homicide, accident or undetermined.

(2) Cause of death is the medical finding or findings responsible for the death.

(3) An attended death is a death that occurs as a result of natural causes wherein the deceased was either hospitalized during at least a 24-hour period preceding death or under the continuing care of a physician immediately preceding the death.

(4) A psychological autopsy is a forensic investigative tool and its purpose is to assist in ascertaining the manner of death.

(5) Equivocal deaths are instances when the death cannot be readily established as natural, accidental, a suicide or a homicide.

(6) The Office of the Armed Forces Medical Examiner (OAFME) is located at 1413 Research Boulevard, Building 102, Rockville, MD 20850.

b. AR 195-2 requires that the USACIDC conduct an investigation into non-combat deaths where medical authorities cannot determine that death resulted from natural causes. A complete investigation will include the results of any autopsy or similar medical/laboratory tests whether conducted by military or civil authorities. Should a final ROI be issued prior to obtaining these results, a

supplementary ROI (see paragraph 7-16) will be prepared when the results are available (see paragraph 4-1 7a(9)).

c. The USACIDC will be responsible to investigate all deaths that occur on a military installation except attended deaths. Attended deaths may be investigated by the USACIDC when deemed appropriate by a CID supervisor. Hospice deaths are considered attended deaths when the USACIDC element was notified of the hospice situation by a recognized hospice representative at least 24 hours in advance of the death.

d. All reported deaths, which are within the investigative responsibility of the USACIDC, will be reported by initial/SSI and recorded by ROI. All such investigations will be conducted as though the death were a homicide.

e. All equivocal deaths and apparent or suspected suicides of Army sponsors or their immediate family members will be reported by initial/SSI, regardless of location of incident. Those deaths not within the primary investigative responsibility of the USACIDC may be finalized by under the provisions of paragraph 4-17.

(1) All equivocal deaths and apparent suicides or suspected suicides will be initially reported/listed as "undetermined death" using the offense code 5H9B.

(2) The investigative summary of the initial/SSI report will describe the events of the death and the results of the preliminary investigation, which may indicate the probable or likely manner of death as a suicide.

(3) Psychological autopsies will not be routinely requested by CID elements. If the OAFME has not made a determination and the SAC, operations officer or Forensic Science Officer (FSO) cannot identify the manner of death after a thorough investigation, an interim report, with all exhibits and an OAFME Contributor Worksheet (see paragraph 5-21(f) and Figure 5-31), will be forwarded to the OAFME. If the OAFME can determine the manner of death, a consultation report will be returned to the submitting office, and a status/SSI or final ROI will be prepared listing the appropriate offense and offense code. If the OAFME requires additional information to determine the manner of death, the OAFME may request the Army Medical Department to conduct a psychological autopsy. The completed psychological autopsy will be returned to the OAFME for consideration in determining the manner of death. The OAFME will submit a final determination to the requesting office and a status/SSI or final ROI will be prepared listing the appropriate offense and offense code.

f. OAFME Contributor Worksheet (Figure 5-31). Submissions to the OAFME will be accompanied by a Contributor Worksheet, which is self-explanatory and will reflect the category of the requested review.

(1) Check block A if the decedent was an active duty U.S. military member at the time of death.

(2) Check block B if the decedent was not active duty, but the SAC, OPS or FSO requests a medicolegal review.

(3) Check block C if the submission pertains to an open investigation and active assistance from the OAFME is requested to address specific concerns.

g. Refer to paragraph 8-15 for special distribution requirements for death investigations.

h. The investigative summary section of each initial/SSI will include the following information, if known:

(1) What, if any, resuscitation efforts were performed and duration.

(2) Any known medical problems and medications found with the deceased that may relate to the cause of death.

(3) The name and location of the pathologist who will or did conduct the autopsy. For circumstances permitting the autopsy to be conducted at military medical centers, see paragraph 4-4, AR 40-2, and chapter 6, AR 40-31.

i. Except for justifiable homicide investigations and suicides, if the death was not the result of a criminal act or omission or medical authorities determine that a death was the result of natural causes, and no other offenses are involved, the investigation will be terminated and a final (C) and will be prepared under the provisions of paragraph 4-17a(9).

j. In those investigations where it is determined that a death resulted from a criminal act or omissions on the part of any person, living or dead, that person will be listed as the subject.

k. Aircraft accidents will be investigated by the National Transportation Safety Board and Army aviation authorities. Normally, the USACIDC will not become involved in any phase of those investigations unless criminal acts are uncovered during their investigation. In those cases, the USACIDC will initiate an investigation.

l. Fatal traffic accidents and other fatal accidents that occur off a military installation involving DA civilian personnel while in the performance of official duties or active duty U.S. Army service members (on or off duty) will be reported by ROI (e.g. initial, joint, collateral). If, based on investigations by the responsible law enforcement agency, a DA civilian or Army service member committed a traffic or criminal offense (e.g., negligent homicide, driving while intoxicated,

reckless driving, etc) which caused or contributed to the fatal accident that person will be listed as a subject of the ROI for the appropriate offense(s). This reporting requirement exists regardless of the DA civilian's or Army service member's physical condition (e.g., deceased), or a decision by civilian authority not to cite the individual for the appropriate offense(s) in their report because of subject's deceased status. Any occupant of any vehicle involved in an accident who sustains a grievous bodily injury will be listed as a victim of the appropriate offense(s) that caused the injury. For the purpose of this paragraph, grievous bodily injury does not include minor injuries, such as a black eye or a bloody nose, but does include fractured or dislocated bones, deep cuts, torn members of the body, serious damage to internal organs, and other serious bodily injuries.

m. All death investigations will be fully coordinated with other command elements and locally established installation working groups. The CID unit should be aware of the group's activities and ensure that the USACIDC actively participates in any meetings which are held.

n. In all cases in which the USACIDC initiates a death case investigation, a Casualty Liaison Officer (CLO) will be appointed by the district, field or equivalent office commander. The CLO will become familiar with the provisions of AR 600-8-1, Army Casualty Operations /Assistance/Insurance, with particular attention to paragraphs 4-1, and chapter 7 of that regulation. The name of the CLO, along with commercial and military telephone numbers, will be immediately provided to the supported Casualty/Mortuary Affairs Office for inclusion in the DA casualty message. The initial/SSI to HQUSACIDC will include the same information.

(1) In CONUS death investigations, the CLO will actively participate with the installation/community casualty working group to collect information, to assist in resolving discrepancies within the working group and to provide a brief summary of the incident based on factual data. The CLO will contact the Casualty Assistance Officer (CAO) in a timely manner to facilitate future briefings. The CLO will brief, as a minimum, the CAO and the chairperson of the installation/community casualty working group, on significant developments during the investigation to ensure they have the most current and accurate information. The CLO will provide only factual information and will not offer opinions or suppositions pertaining to any aspects of the investigation. The CLO will not disclose information which would compromise the investigative effort, deprive an individual of a fair trial, or which would be an unwarranted invasion of an individual's privacy. All information released to the installation/community casualty working group or other non-investigative entity during a death investigation will be released only by the CLO. In the event a CLO is replaced during an active investigation, the newly designated CLO will notify the chairperson and CAO of the change. Responsibilities of the CLO extend to the primary next-of-kin (PNOK) and the secondary next-of-kin (SNOK). The line of succession in determining the PNOK is explained in paragraph 3-7, AR 600-8-1. The SNOK is defined as any NOK other than the PNOK. The CLO will be

responsive to either or both the PNOK and the SNOK. The next-of-kin (NOK) includes, but is not limited to, the following relationships:

(a) spouse, even if a minor;

(b) sons or daughters;

(c) parents;

(d) brothers or sisters;

(e) grandparents;

(f) other relatives to the individual in accordance with the laws of the deceased's domicile;

(g) persons in loco parentis.

If the NOK contacts the CLO personally, the CLO will be responsive to the concerns of the NOK and will answer questions and address issues of the NOK in a professional manner to the fullest extent possible without impeding or endangering successful completion of the investigation. In those instances in which a family member is suspected or implicated in the investigation, the CLO/operations officer/commander must make a prudent and judicious decision in the release of information addressing the concerns of the NOK, yet maintaining the integrity of the investigation. The CLO will brief, as a minimum, the CAO and the chairperson of the installation/community casualty working group, on the results of the investigation once the investigation is completed. The responsibilities of the CLO in a criminal death investigation will continue until the investigation is finalized and forwarded to the SJA for disposition of the offender. At that time, the USACIDC CLO relinquishes all responsibilities for that particular investigation to the Victim/Witness Coordinator for the SJA office. The responsibilities of the CLO in non-criminal death investigations (i.e., suicide, accidental, natural, undetermined) continue until all issues and concerns a re reasonably resolved.

(2) In death investigations in which the casualty occurs OCONUS and the NOK resides in CONUS or in another overseas command, or in those instances in which the casualty occurs in CONUS and the NOK resides OCONUS, two CLOs will be appointed. One will be appointed at the office initiating the investigation (designated as the initiating office CLO) and another at the office supporting the installation providing casualty assistance to the NOK (designated as the receiving office CLO). The initiating office CLO will coordinate with the local casualty affairs office and identify the Casualty Area Command (CAC) or installation which will be extending casualty assistance to the NOK. The initiating CLO will expeditiously notify the USACIDC field element supporting that CAC or

installation of the casualty. The field element receiving notification of the casualty will notify the district, field, or equivalent office commander to appoint a CLO at the receiving office for that investigation. The receiving CLO will promptly notify the supported Casualty/Mortuary Affairs Office of the local CLO's appointment. The initiating office CLO will ensure the receiving office CLO is appropriately briefed on all significant aspects of the investigation. The receiving element will be on distribution for the initial/SSI, as well as all subsequent reports. The receiving office CLO, if contacted by a CAO or by the NOK, will answer questions and address issues concerning the investigation in the same manner described in paragraph 5-21l(1). The initiating field element is responsible for the content of all information released to the CAO or NOK by the receiving element.

(3) The USACIDC field element commander, as a member of the installation/community casualty working group, plays a primary role in the functions of the group, especially when USACIDC has primary investigative jurisdiction of a death investigation. Although the USACIDC commander is not responsible for monitoring the functions of the casualty working group, it is paramount that the USACIDC field element commander, when it is observed that the working group is not functioning to serve the best interests of the NOK and/or the Army, address those concerns to the chairperson of the casualty working group.

o. IAW ALARACT 019/01, the Casualty Memorial Affairs Operation Center (CMAOC) may establish, on a case-by-case basis, a Next of Kin (NOK) notification team for some fatal training accidents. Normally, this team will be formed in response to Class A accidents (fatal) as defined in AR 385-40, Army Accident Reporting and Records, 1 Nov 94. The USACIDC Casualty Liaison Officer (CLO) will fully cooperate with such teams when established by providing investigative details deemed appropriate. The information provided, however, may be restricted if release would adversely affect the investigation or jeopardize the successful resolution or prosecution of the investigation. When a NOK notification briefing team is identified, the USACIDC CLO will initiate contact with the team commander and provide assistance as requested and within USACIDC guidelines. Requests for inclusion of USACIDC personnel to augment, and/or travel with, a NOK notification briefing team will be forwarded to the CID Group for approval prior to providing the requested support.

5-22
Missing persons

a. The USACIDC, IAW paragraph 4-9(a)(1) of this regulation, will conduct an investigation on all incidents occurring on an Army installation when a person is missing due to unusual or suspicious circumstances; or when indications of foul play exist; or when the person is missing for no apparent reason; or when the circumstances manifest a radical deviation from the missing person’s normal

behavior (Figure 5-32, Missing Persons Protocol/Checklist). The investigation of soldiers or their family members determined to be missing under unusual or suspicious circumstances which occur off the installation will be undertaken in conjunction with the responsible civilian law enforcement agency and will be reported as a joint or collateral ROI, as appropriate. (ALCID 004-03).

b. Upon notification of a person missing within the parameters of paragraph described above, an INI/SSI, JOINT/SSI, or COLLATERAL/SSI will be dispatched IAW in paragraph 7-10, including the appointment of a single USACIDC point of contact for that investigation comparable to the casualty liaison officer in a death investigation. If, during the investigation, the missing person is located or verifiable information is developed identifying the person's whereabouts, and no other circumstances warrant USACIDC involvement, the investigation will be terminated IAW paragraph 4-17(a)(6) of this regulation. (ALCID 004-03)

c. Missing persons ROIs will be fully investigated as a suspected death investigation. Missing person investigations should continue until all reasonable leads have been exhausted. All missing persons will be entered into the National Crime Information Center (NCIC) IAW paragraphs 5-36b(6) and 5-36e of this regulation. Missing persons subsequently located will be promptly removed from the NCIC. (ALCID 004-03)

d. All investigations involving missing persons having access to classified defense information will be fully coordinated with the supported military intelligence activity. (ALCID 004-03)

e. Commanders, operations officers, and special agents-in-charge must make a judicious decision in evaluating the criteria outlined in this policy guidance when initiating a missing person's investigation. It is imperative that the USACIDC investigate suspicious and legitimate incidents of missing persons, without becoming a clearinghouse for locating runaway juveniles, estranged spouses, or soldiers in absent-without-leave or deserter status. (ALCID 004-03)

f. The following offense codes have been entered in the ACIRS database and will be used to report all incidents of missing persons (ALCID 004-003):

9P - Missing persons

9P1 - Military/sponsor

9P1A - Officer

9P1B - Enlisted

9P2 - Family member

9P2A - Spouse

9P2B - Son/step-son

9P2C - Daughter/step-daughter

9P2D - Other family members

9P3 - Others

5-23
Reporting of casualties during operations other than war

a. Definitions:

(1) Casualty: Any person who is lost to the organization by reason of having been declared beleaguered, besieged, captured, dead, diseased, detained, duty status-whereabouts unknown, injured, ill, interned, missing, missing in action, or wounded.

(2) Casualty area command: A command assigned operational responsibility for the area in which the casualty occurs and which has casualty reporting responsibilities to the PERSCOM Casualty Operations Center.

(3) Hostile casualty: A person who is the victim of a terrorist activity or who becomes a casualty "in action." "In action" characterizes the casualty as having been the direct result of hostile action, sustained in combat or relating thereto, or sustained going to or returning from a combat mission provided that the occurrence was directly related to hostile action. Included are persons killed or wounded mistakenly or accidentally by friendly fire directed at a hostile force or what is thought to be a hostile force. However, not to be considered as sustained in action and not to be interpreted as hostile casualties are injuries due to the natural elements, self- inflicted wounds and, except in unusual cases, wounds or death inflicted by a friendly force while the individual is in absent- without-leave, deserter, or dropped from the rolls status or is otherwise voluntarily absent from a place of duty.

(4) Non-hostile casualty: A person who becomes a casualty due to circumstances not directly attributable to hostile action or terrorist activity.

b. The reporting of hostile casualties which occur during operations other than war is the responsibility of the supporting Casualty Area Command. The USACIDC will not normally investigate or report casualties resulting from hostile (combat) action. However, the USACIDC may investigate and report casualties

resulting from hostile action (e.g., friendly fire) on a case-by-case basis either (1) upon approval by the senior USACIDC supervisor on location, if such investigation would better serve the interest of the Army and/or U.S. Government, or (2) upon a request from the senior U.S. military commander on location. The investigation of casualties resulting from hostile action will be initially reported by "initial/SSI" ROI with subsequent "status/SSI" reports dispatched as appropriate. The investigation and reporting of deaths resulting from hostile action is not to be inferred as supplanting the normal reporting responsibilities of the supporting Casualty Area Command.

c. Casualty reporting includes not only the reporting of Department of the Army personnel but may also include casualties of other U.S. military service personnel.

d. Investigation/reporting of non-hostile casualties within the investigative purview of the USACIDC remains the responsibility of the USACIDC.

5-24
Supervisory considerations for death investigations

a. Basic procedures for investigating reports of death are outlined in Army Field Manual 19-20, Law Enforcement Investigations. This manual is the guide for the special agents in applying their technical skills and techniques. Supervisors should ensure that the investigation is timely and thorough. The implementation of local initiatives to ensure quality investigations is encouraged.

b. In equivocal deaths, a psychological autopsy may be requested by the OAFME (paragraph 5-25e (3)) upon submission of a USACIDC interim report and OAFME Contributor Worksheet (paragraph 5-21n). Reports of psychological autopsies and the OAFME Consultation Report will be included as an exhibit in the ROI.

c. Autopsy authority for soldiers, unknown individuals, or individuals who die on army installations.

(1) Under 10 US Code 1471, Forensic Pathology Investigations, the Armed Forces Medical Examiner (AFME) is authorized to conduct or approve the conduct of a medicolegal death investigations and to authorize autopsy examinations when it appears that the decedent was killed or that, whatever the cause of the decedent's death, the cause was unnatural; the cause or manner of death is unknown; there is reasonable suspicion that the death was by unlawful means; it appears that the death resulted from an infectious disease or from the effects of a hazardous material that may have an adverse effect on the military installation or community involved; or the identity of the decedent is unknown; or the decedent was found dead or died at an installation garrisoned by units of the

armed forces that is under the exclusive jurisdiction of the United States; or the decedent was a member of the armed forces on active duty or inactive duty for training. The OAFME authority extends to civilian dependents of service members who die outside the United States. Authority for the military to accomplish or request an autopsy on other civilian personnel will vary according to state law or the law of the foreign country in which the death occurs. Liaison with the local judge advocate's office should be performed in advance to preclude potential legal problems that may arise when CID desires an autopsy of a civilian. Loss of valuable time will be minimized if supervisors explore in advance the various avenues for having an autopsy performed on a civilian victim or a soldier off a military installation.

(2) In accordance with AR 40-2, Army Medical Treatment Facilities, General Administration, Medical Treatment Facility (MTF) commanders may authorize autopsies performed on the remains of soldiers who die on active duty. In CONUS, if applicable state laws authorize the performance of an autopsy, the MTF commander may order the autopsy without the consent of the spouse or NOK. These autopsies, according to AR 40-2, may be performed when:

(a) It is considered necessary to determine the true cause of death, or

(b) Death occurs while the soldier is serving as an aircraft crewmember in a military aircraft (autopsy in this instance is mandatory).

(3) In the case of a death of any person held as a detainee under the custody of the U.S. Army, the commander of the detention facility (or of the death did not occur in a facility, the commander of the unit exercising custody of the individual) will immediately report the death to Army law enforcement authorities. For the purposes of this policy, a detainee is defined as, "any person captured or otherwise detained by an armed force. The detention need not occur at a MP controlled detention facility and may include checkpoints and cordon and search operations." Once notified of the death, the responsible CID element will expeditiously contact the Office of the Armed Forces Medical Examiner (AFME), which will determine whether an autopsy will be preformed. Upon determination of death, the controlling CID element will ensure the remains of the decedent are placed in a clean body bag and secured. The remains will not be washed and all items on or in the body will be left undisturbed except for weapons, ammunition, and the other items that pose a threat to human life. The body will not be release from US Custody without written authorization or prior approval from the Armed Forces Medical Examiner. Determination of the cause and manner of death in these cases will be the sole responsibility of the Armed Forces Medical Examiner or other physician designated by the Armed Forces Medical Examiner.

d. Autopsy authority for civilians. Authority for the military to accomplish or request an autopsy on civilian victims will vary according to state law or the law of the foreign country in which death occurs. Liaison with the local judge

advocate's office should be performed in advance to preclude potential legal problems which may arise when an autopsy of a civilian is desired by CID. Loss of valuable time will be minimized if supervisors explore in advance the various avenues for having an autopsy performed on a civilian victim or a soldier off-post.

e. Casualty working group. Installation casualty working groups will meet as often as necessary, according to AR 600-8-1, Army Casualty and Memorial Affairs and Line of Duty Investigations, to review required action, exchange information and ensure that the next-of-kin have the most accurate information and support available. One purpose of this group is to ensure that the Army speaks with one voice. The CID commander/supervisor or the CLO will be a member of this working group.

f. Medical record review. Medical records may contain information not easily understood by the CID supervisor or special agent. A list of authorized medical abbreviations and symbols to be used in medical records is contained in AR 40-66, Release of Medical Information. Identification of prescription drugs prescribed for or taken by the victim at the time of death should be noted and recorded in the ROI, along with information on any chronic or acute illness or disability.

g. Confidentiality of medical information. Any CID personnel seeking medical information about a patient must request it in writing from the medical treatment facility commander, according to AR 40-66. DA Form 4254-R, Request for Private Medical Information, will be used for such requests. In certain situations, such as cases of rape, sexual assault, child abuse and death, the need for information may be urgent. In these cases, both the request for information and permission for disclosing it may be given verbally.

h. Release of information to the media (paragraph 5-59).

i. Property of deceased individuals.

(1) Paragraph 19-3a, AR 638-2 states that personal effects found on remains will normally be collected and inventoried at the first mortuary affairs collection point to which the remains are delivered. However, in unattended deaths occurring in CONUS and OCONUS the remains are often transferred to another location for an autopsy and the initial mortuary affairs collection point is either by-passed or because of the need to safeguard evidence the personal effects are not removed from the remains. Thus, the remains arrive at the autopsy suite with personal effects still on or with the remains.

(2) Personal effects having potential value as evidence do not pose a problem as they are removed and accounted for on a DA Form 4137, Evidence/Property Collection Record and placed in the evidence room. It is the personal effects, which remain with the body and have no evidential value that have the potential of becoming lost or stolen. In order to ensure proper accountability of all personal

effects remaining on the deceased at the time of autopsy and prevent miscommunication between mortuary affairs personnel and CID Special Agents, the following guidance is effective immediately:

(a) The senior special agent attending the autopsy will coordinate with the pathologist and/or mortuary affairs personnel regarding the correct disposition of personal effects accompanying the remains. It will be pointed out that CID will collect some of the effects, as evidence, and some will not be collected. Those items having no evidential value still need to be accounted for under the provisions of AR 638-2, by mortuary affairs personnel. The senior special agent will ensure the mortuary affairs personnel and the pathologist clearly understand what items are being obtained as evidence and what items are not being collected.

(b) Special agents will not depart the autopsy suite until it is clear, in everyone’s mind, which items of personal property are specifically being accounted for and by whom. Special agents are not required to remove items of personal effects solely for safekeeping.

(c) Agents will not knowingly allow items of personal property to become lost or susceptible to theft.

j. Case review. Coordination with FSOs should be considered for investigative plans and when providing investigative guidance. An independent review by someone not close to the investigation may be beneficial. Sources for assistance should be identified before the need arises. If expertise is not available locally, then a formalized system for requesting additional assistance should be established.

5-25
Adult private consensual sexual misconduct (APCSM)

a. Definitions

(1) "Sexual misconduct" is a sexual act or acts in violation of Title 10, Chapter 47, United States Code (Uniform Code of Military Justice (UCMJ)) that occur between consenting adults, in private, whether on or off a military installation. It does not include any sexual act or acts that involve allegations of force, coercion, intimidation, abuse of position or rank, fraternization, persons under the age of 16 years, or conduct that relates directly to applicable security standards for access to classified information.

(2) "Sexual orientation" is an abstract sexual preference for persons of a particular sex, as distinct from a propensity or intent to engage in sexual acts. In

and of itself, sexual orientation towards homosexuality or bi-sexuality is not a violation of the UCMJ.

(3) "Commander" is a commissioned or warrant officer who, by virtue of rank and assignment, exercises primary command authority over a military organization or prescribed territorial area that under pertinent official directives is recognized as a command; or a civilian supervisor in a comparable position who is outside a Defense Criminal Investigative Organization (DCIO) and is authorized to request an investigation or act on the results of an investigation by a DCIO.

(4) “Credible information,” for the purpose of evaluating allegations of APCSM, is defined as information, considering its source and all surrounding circumstances, that supports a reasonable belief that a service member has engaged in sexual misconduct. Credible information consists of articulable facts, not just a belief or suspicion.

(5) “Non-ROI activity” refers to any USACIDC activity not associated with the conduct of an on-going ROI (e.g., information received from a source, information collected as raw data, telephone complaints, congressional inquiries, etc).

(6) For the purpose of this policy, an APCSM allegation is considered “germane” to an ROI if the incident is closely associated to the matter under investigation (primary offense). For example, an allegation of an adulterous relationship discovered during the investigation of an alleged suicide may be germane to establishing the subject’s emotional state at the time of death. An adulterous relationship discovered during the investigation that occurred 20 years ago would most likely not be germane to the alleged suicide.

(7) “Aggravating circumstance”, as it relates to this policy, is any APCSM allegation that:

(a) is detrimental to good order and discipline and/or

(b) involves senior personnel as defined in paragraph 5-4(a) of this regulation and/or,

(c) has media potential and/or

(d) has been requested by a field grade commander

b. Policy

(1) The USACIDC will not conduct investigations to determine a service member’s sexual orientation (e.g., heterosexual, homosexual or bi-sexual).

(2) The USACIDC will not conduct any inquiries where the allegations consist solely of a verbal admission from a service member of his/her sexual orientation.

(3) Normally, the USACIDC will not conduct an investigation of APCSM when it is the only allegation involved. An investigation of an APCSM-only allegation may be initiated only if approved by the CG, USACIDC in compliance with subparagraph 5-25c below.

(4) When an allegation of APCSM is investigated IAW the procedures in subparagraph 5-25c, the investigation will be limited to the factual circumstances directly relevant to the specific sexual misconduct allegation. These investigations will be conducted in an evenhanded manner, without regard to the service member's sexual orientation.

c. Procedures (See Figure 5-30)

(1) When a commander refers an APCSM allegation or an APCSM allegation is discovered during non-ROI activity, the USACIDC unit receiving the allegation will make an independent determination, based on the presented facts and evidence, whether credible information of sexual misconduct exists. A preliminary investigation will not be initiated to assist in this determination. If credible information does not exist or if APCSM is the only offense involved and does not include any aggravating circumstance, the matter will be referred back to the commander, without action, for disposition. If there are aggravating circumstances or if the commander insists upon an investigation, the USACIDC unit will forward the matter through its chain of command to HQUSACIDC for a decision prior to the initiation of any investigation, in accordance with paragraphs 5-25c(4) and (5) below. If a commander withdraws his request for investigation, the matter need not be forwarded to HQUSACIDC.

(2) If a referred or developed APCSM allegation is not the only offense involved, the USACIDC unit receiving the allegation will make a determination whether the APCSM allegation is germane to either an on-going ROI or to the further investigation of the other non-APCSM offense(s). Consultation with the supported SJA is encouraged. If the APCSM allegation is not germane to an investigation of the other offenses, then the procedures in paragraph 5-25c(1) above will be followed. If the APCSM allegation is germane to the investigation of other offenses, then the procedures in paragraph 5-25c(3) below will be followed.

(3) If a credible act of APCSM by a service member is discovered during the conduct of an ROI, the USACIDC unit will make a determination whether the APCSM allegation is germane to the furtherance of investigation of the primary non-APCSM offense(s). Consultation with the supported SJA is encouraged. If the APCSM allegation is not germane to the investigation of the other offenses, then the procedures in paragraph 5-25c(1) above will be followed. If the APCSM allegation is germane to the investigation of other offenses, then the APCSM

allegation will be investigated only to the extent necessary to develop the primary offense(s). Under this circumstance, rights advisements will be administered when appropriate, but the APCSM offenses will not be listed in the subject and/or victim blocks of the ROI, unless prior approval of the CG, USACIDC was obtained under the provisions of paragraphs 5-25c(4) and (5) below. APCSM allegations determined to be germane to an ROI and investigated to the extent necessary but not listed in the subject and victim blocks, will be referred to the action commander for disposition upon completion of the ROI.

(4) When seeking a CG, USACIDC decision whether to conduct an investigation of an APCSM allegation because of aggravating circumstances or a commander's request in accordance with paragraphs 5-25c(1) or (3) above, all available information will be forwarded through USACIDC command channels to the Deputy Chief of Staff for Operations (DCSOPS), HQUSACIDC, ATTN: CIOP-OP. The DCSOPS will review and forward the matter to the CG, USACIDC to determine whether to initiate an ROI. No ROI or preliminary investigation will be initiated without prior approval of the CG, USACIDC. If immediate approval is required during other than normal duty hours, the information will be forwarded to the HQUSACIDC Staff Duty Officer who will notify the DCSOPS of the request.

(5) Any APCSM allegation approved for investigation by the CG, USACIDC will include appropriate rights advisement to those involved, and the APCSM offenses will be listed in the subject and victim blocks of the ROI. Any APCSM allegation disapproved for investigation by the CG/DCO, USACIDC will be referred to the appropriate action commander(s) and closed in the files of the originating office without further action.

(6) When referring an APCSM allegation to a commander for action, the following entry will be used: IAW the investigative guidelines for sexual misconduct outlined in DoDI 5505.8, AR 600-20 and CIDR 195-1, the referenced adult private consensual sexual misconduct is not within the normal purview of CID and is referred to the commander for disposition. This phrase will be inserted in the summary paragraph of any ROI in which APCSM is referred to a commander, or in any memorandum that refers or returns an APCSM allegation to a commander.

(7) In accordance with DODI 5505.8, the CG, USACIDC may delegate decision-making authority over APCSM requests to the Deputy Commander, USACIDC.

d. This policy is an exception to paragraphs 4-7 and 4-9, which require the initiation of a criminal investigation based on credible information that a crime has occurred and the USACIDC has investigative responsibility.

5-26
Self-confessed offenders

a. When a self-confessed offender refuses to provide information about the offense sufficient to conduct an investigation to substantiate that the offense occurred, a thorough preliminary investigation, if warranted, will be conducted. If no other credible information is developed, the sequence number action will be completed and a criminal intelligence report submitted.

b. The individual's commander, and if appropriate, the local military intelligence activity will be informed of the results of the preliminary investigation.

c. If the individual furnishes specific information as to names, places, and dates of the criminal offense, and the USACIDC has investigative responsibility, an ROI will be initiated. However, see paragraph 5-25 for guidance on consensual sexual misconduct crimes.

5-27
Terrorism and major disruption

a. Appropriate USACIDC units will collect, analyze, and disseminate criminal intelligence on terrorist threats to appropriate police, DoD, and DA agencies.

(1) Local commanders and provost marshals/security officers will be kept advised of all terrorist threats in their areas of responsibility and will be provided updated information as it is developed.

(2) All information concerning terrorist threats will be coordinated with local military intelligence, FBI, police, and other agencies as appropriate.

(3) Terrorist threats will be reported by criminal information report in accordance with chapter 18 and SSI in accordance with paragraph 7-10. Also, refer to chapter 16, Combating Terrorism Program.

b. Appropriate USACIDC units will investigate major disruptions on installations. Included are threats or attempts to commit such acts as kidnapping, blackmail, bombings, hijacking, ambushes, sabotage, major weapons thefts, extortion, assassination, and taking of hostages.

(1) In cases of sabotage, local military intelligence and the FBI will be notified and kept abreast of the investigation.

(2) Investigation of major disruptions will be reported by ROI in accordance with chapter 7.

c. Appropriate USACIDC units will also support local commanders and provost marshal/security officers by providing the following:

(1) Advice in the form of personal vulnerability assessment. Assessments will be conducted to deal with specific targets of opportunity and in support of protective service missions.

(2) Training assistance concerning counter terrorist measures.

(3) Trained CID hostage negotiators. Appropriate USACIDC units will develop and monitor plans for identification and notification of CID agents qualified to support terrorist/hostage situations.

(4) Assistance in the preparation of counter terrorist/hostage plans which integrate CID within the installation/community counter terrorist hostage plan.

d. For additional information on personal vulnerability assessments, terrorism and major disruptions, see AR 190-52, CID Pamphlet 195-7, and chapters 15 and 16 of this regulation.

5-28
U.S. Government owned weapons

a. Preliminary investigations will be conducted in instances involving lost/missing U.S. Government weapons and ammunition when the amount exceeds thresholds established in AR 190-11. If no credible information indicating theft is established, no ROI is required.

b. All thefts of the following will be investigated by CID:

(1) All weapons (less bayonets, etc.) and munitions (not artillery or grenade simulators, etc.).

(2) Ammunition larger than .50 caliber (less shotgun).

(3) Shotgun and other small arms ammunition of .50 caliber and less when amounts exceed 1,000 rounds; and .22 caliber rim fire in amounts exceeding 10,000 rounds.

5-29
Coordination with Staff Judge Advocate (SJA)

a. Supervisors will ensure that reports of investigation are coordinated with appropriate SJAs to determine if the investigation is complete and sufficient for

legal purposes. For investigative purposes, legal sufficiency is primarily concerned with whether:

(1) An individual is properly listed as a subject.

(2) The offense is properly shown as founded.

b. Other aspects of investigations of mutual concern to USACIDC personnel and SJA include whether:

(1) The USACIDC has investigative responsibility and authority over the subject matter under investigation.

(2) All appropriate criminal offenses have been considered.

(3) The appropriate victim has been listed.

(4) Investigative leads exist which require the investigation to prove or disapprove the listed offense(s).

c. Special agents conducting or directing investigations will maintain coordination concerning their investigations with appropriate judge advocates. This responsibility is distinct from the need to maintain continuing liaison with commander s or other criminal investigative agencies having an interest in the case.

d. Legal review of investigative efforts and facts resulting there from is required prior to the designation of an individual as a subject in a final report of investigation.

e. Early coordination with SJA is appropriate when:

(1) There is a question regarding the precise nature of alleged criminal conduct.

(2) Elements of proof are uncertain.

(3) It is questionable whether credible information exists for listing an individual as a subject.

(4) Investigative activity involves sensitive legal issues such as search and seizure, interception of wire and oral communications, detention of civilians, or off-post investigative effort.

f. The SJA will be kept informed of a development which might affect prosecution of any subject (e.g., pending reassignment of witnesses, obstruction

of justice efforts, false swearing, or false official statement or facts indicating lack of court-martial jurisdiction over the subject matter).

g. A USACIDC unit may, at any time, seek legal advice/guidance directly from the USACIDC major subordinate command judge advocate (JA). This coordination should not be used to avoid the requirement to obtain legal review of investigations by the SJA of supported commanders. Situations in which the USACIDC major subordinate command

important that briefings be concise while meeting the needs of the individual being briefed.

c. The senior officer being briefed needs to know what the investigation concerns and what impact, if any, it is going to have on his/her command. Minute details of the investigation need not be covered.

d. Agents/supervisors conducting the briefing should discuss the who, what, when, where, and how of the investigation in enough detail to provide the senior officer with information he needs to know without going overboard on the specific details. More important, the person conducting the briefing should be familiar enough with the investigation to answer questions that arise as a result of the briefing. The ability to answer these questions, at the time of the briefing, will save much time later on for the senior officer and the agents conducting the investigation.

e. A short, properly presented briefing that covers the information required will indicate to the person being briefed that the demands on his/her time are appreciated and that the briefer has taken time to prepare a concise, professional presentation.

5-33
General

a. All CID special agents and supervisors at all levels will make maximum use of specialized investigative expertise.

b. Within the USACIDC, a wide range of special investigative assistance is available and should be requested when needed. Telephonic requests are authorized when required by time constraints.

(1) Polygraph support will be requested in accordance with paragraph 5-33.

(2) Normal USACIL support will be requested in accordance with AR 195-2, AR 195-5, and chapter 24 of this regulation. Note: The primary offense code for the investigation being conducted will be annotated on all crime lab examination requests submitted to the USACIL. The offense code will be placed in block 1 (contributor case number) immediately following the sequence/ROI number.

(3) Crime scene support by USACIL personnel will be requested through the USACIL headquarters.

(a) Crime scene USACIL support is costly both in travel expenses and in time. It should not be requested when the required expertise is reasonably

available from another source or when the seriousness of the offense will not justify the cost. However, when there is a highly complex crime scene in conjunction with a serious crime, and in the opinion of the responsible CID supervisor, USACIL support is required for adequate processing and evaluation of the crime scene, a re quest should be forwarded.

(b) If the USACIDC major subordinate commander agrees with the propriety of the request, the USACIL Commander will be provided the facts supporting the request, the nature of the support requested, and a fund cite. The USACIL commander will either:

1. Provide the requested support, or

2. Deny the request, informing the requesting commander of the reason for the denial.

(c) Chapter 24 of this regulation provides for travel by USACIL personnel.

(4) Requests for other specialized investigative support by special agents (e.g., homicide, arson, linguistics expertise) will be submitted to the USACIDC major subordinate commander of the requesting USACIDC unit.

c. Outside USACIDC. CID supervisors may utilize the assistance of any experts, military or civilian, within their area. However, the following criteria apply:

(1) The prior approval of the USACIDC major subordinate commander must be obtained, if the assistance is reimbursable.

(2) Effective 1 October 1995, the U.S. Army Criminal Investigation Laboratory (USACIL) will arrange and fund contractual support for forensic services that are outside their capability. The determination that the desired forensic services are outside the USACIL capability will be made by the USACIL either through direct examination of the evidence or through discussion with the requesting field element. Once the need for external forensic service is determined, the district commander will be informed of the known or projected cost of the external forensic service and will confirm its operational necessity at the cited cost before the USACIL will execute the service contract. Telephonic confirmations of operational necessity are authorized. Upon confirmation of the operational necessity, the evidence will be forwarded to the USACIL who will examine the evidence and determine the forensic processing plan prior to forwarding it to the external entity for analysis. The USACIL will be responsible for ensuring that the contracted services are performed satisfactorily before the evidence is returned to the requesting field element. Field elements should refer any queries from an external contractor about the contracted evidence processing and evaluation to the USACIL. Under exceptional circumstances, the USACIL may authorize direct transfer of the evidence between the requesting field element and the contractor.

(a) Under the current system, which remains in effect until 1 October 1995, field elements requesting forensic services outside the USACIL capabilities are required to arrange their own contracts via the local contracting office. Under the new system, Once the district commander of the requesting field element confirms the operational necessity of the proposed forensic services, the USACIL will prepare and submit the required contract paperwork; fund the contracted services from their operating budget; and ensure that the contracted services were performed. District commanders are expected to exercise prudent decision making when confirming the operational necessity of forensic services outside the USACIL capabilities.

(3) If audit support to an investigation is required, a written request to the appropriate audit element will be provided in a timely fashion so as to give the audit organization as much advance notice as possible. A list of U.S. Army Audit Agency (USAAA) district offices is reflected in appendix H. A list of Defense Contract Audit Agency (DCAA) regional offices is presented in appendix I. The request for audit support will contain the following information:

(a) A statement of the problem containing sufficient detail to identify specific audit tasks required. Informal contact with the audit organization may be necessary to develop the specific requirements for the audit.

(b) The desired starting date and anticipated completion date for the audit.

(c) The location where the audit is to be conducted.

(d) Any other information which may assist in determining the scope of the audit and any potential impact on existing audit schedules.

(e) Care must be taken to ensure the audit request does not involve non-professional services or functions which would fall outside of the normal auditing procedure.

d. When a USACIDC commander desires non-CID specialized assistance from outside the commander's area, the request will be submitted to the USACIDC major subordinate command of the requesting unit.

e. Dun and Bradstreet (D&B) reports can be requested in writing through USACIDC, ATTN: CIOP-IN, or by telephone. If five or more reports are requested, submit the request in writing by letter or message. Some of the types of reports available through D&B are:

(1) Business Information Report (BIR). The BIR is a narrative report available for individual businesses. It provides details on companies and management

background, product line, function and facilities, finances, and a survey of cur rent trade payments.

(2) Payment Analysis Report (PAR). The PAR is a summary compilation and comparison of the payment record of the business. It contains an in-depth, 12 month analysis of a company's payment record, compared to other companies in the same line of business and same size range.

(3) Government Activity Report (GAR). The GAR can be very beneficial when looking at specific contract information. The GAR shows the non-tax financial relationship a company has with the U.S. Government. It will identify other relate d companies (branches, subsidiaries, parent) who also have activity with the government. It also includes government transactions such as direct loans or guarantees, status of debts or claims (other than tax matters), contract and grant awards, plus a digest of similar activity with related companies and/or branches.

(4) To maximize this command's investment, each request should be carefully reviewed to ensure that the expense of a D&B report is justified.

f. Financial Crimes Enforcement Network (FinCEN) data may be requested through USACIDC, ATTN: CIOP-IN. See paragraph 18-13d of this regulation.

5-34
Polygraph

a. AR 195-6 (Department of the Army Polygraph Activities), and CIDR 195-28 (Polygraph Activities), provide additional instructions for preparation/sub-mission of polygraph documents and provides for utilization and control of CID polygraph examiners.

b. The Commander, USACIDC, and his designated representatives are authorized to approve the conduct of polygraph examinations in connection with criminal investigations. The designated representatives are:

(1) The Deputy Commander, USACIDC;

(2) the Director, USACRC;

(3) the Chief, Polygraph Division, USACRC.

c. The Director, USACRC, and Chief, Polygraph Division, USACRC, are designated the primary approval authorities authorized to approve polygraph examinations. The major subordinate commanders are only authorized to approve the conduct of examinations when:

(1) The designated approving authorities cannot be reached within a reasonable period of time (not more than a two-hour time period);

(2) when further delays in administering an examination would severely jeopardize the mission.

d. The purpose of a polygraph examination, in connection with a criminal investigation, is to determine whether or not the examinee was involved in or has guilty knowledge of the offense(s) of which the examinee is suspected.

e. Since the results of a polygraph examination are not normally admissible in a judicial proceeding, other reasonably available investigative methods of determining veracity should be attempted prior to requesting a polygraph examination. T his does not preclude the use of the polygraph prior to exhausting all leads during the conduct of the investigation. Final determination as to the appropriateness of a polygraph examination, prior to completion of all reasonable investigative leads, will be referred to authorizing authorities in their respective area of responsibility. The polygraph will not be used as a substitute for aggressive investigative effort.

f. The use of the polygraph is restricted to suspects/subjects of the offense under investigation. Polygraph examinations may be requested of individuals originally considered witnesses or victims in the investigation when evidence is developed to support a reasonable belief that such individuals may have committed the offense of false swearing or false official statement and the special agent is unable, through other means, to determine whether or not they are being truthful. Polygraph authorization officials will review each polygraph examination request on a case-by-case basis evaluating technical and regulatory requirements. Under most circumstances, attempts to resolve criminal issues should be resolved through polygraph testing of the primary suspect of the case.

g. A request for a polygraph examination should be in furtherance of a USACIDC initiated ROI, unless it results from a request for assistance from another agency (i. e., Military Police, Trial Defense Service, supported commander, or for exculpation) to resolve an incident that is not within USACIDC's investigative purview. Polygraph examination requests in support of USACIDC investigative actions not documented under an ROI may be approved by the Director, USACRC or the Chief, Polygraph Division, USACRC on a case by case exception basis. In those instances, a justification (e. g., to establish the reliability of a source; an ROI number is not available at the time of the request; the examination is requested under the provision of Chapter 19; etc.) must be provided in paragraph 2c of the polygraph examination request.

h. Requests for polygraph examinations will not be approved in investigations of an offense for which the maximum punishment under the UCMJ is less than one year confinement or for the offenses of false swearing or making a false

statement when the offense to which the false swearing or false statement pertains is an offense for which the maximum punishment under the UCMJ is less than one year (e.g., false swearing relative to the offense of disobeying the order of a noncommissioned officer). Exceptions will be considered when requests are exculpatory in nature. These are defined as those instances wherein the request for an examination originates by that person or someone acting in his behalf such as an attorney or commander.

i. The polygraph authorization officials identified in paragraph b above, are authorized to approve USACIDC polygraph testing of suspects of Adult Private Consensual Sexual Misconduct when polygraph testing is requested by the supported commander of the examinee. The consideration is in support of the affected Army Commander, rather than support of a USACIDC investigation. Consistent with paragraph 5-25 of this regulation, polygraph support under these circumstances is limited to the conduct of the polygraph examination and the post-test interview of the examinee. No additional investigative activity will be conducted without authorization required by paragraph 5-25 of this regulation.

j. A polygraph examination is not appropriate when relative to a case that is in the process of trial. The post trial conduct of a polygraph examination of convicted offenders, in connection with the offenses of which they were convicted, is not appropriate. Similarly, the polygraph examination of witnesses who have testified in a judicial proceeding is not appropriate for the purpose of verifying or discrediting their previous testimony before the court. The use of the polygraph is not prohibited in support of an open investigation of the offense of perjury.

k. Special agents and their supervisors must identify the possible need for a polygraph examination as early as possible and promptly initiate coordination with the supporting polygraph examiner.

l. It is the responsibility of the investigating special agent to prepare the request for a polygraph examination (See figure 5-5). The supporting polygraph examiner will assist in the preparation of polygraph requests, if needed.

m. The ACIRS CID electronic mail (E-Mail) will generally be used for submission of all polygraph requests. In the event of transmission difficulties or other emergencies, requests may be submitted by facsimile, telephonically or by mail. All telephonic requests must be followed up by an E-Mail request within 24 hours of submission.

n. The conduct of the polygraph examination, including preliminary and post-test phases, is under the control of the polygraph examiner. The special agent investigating the case will monitor the examination and take any written statement made by the examinee. In the event the special agent investigating the case is unavailable, another special agent will be designated to perform the

monitor's functions. Both the agent and polygraph examiner should keep in mind that any statement made by the interviewee in the preliminary and post-test phase, as well as during the examination, may significantly add to the overall investigation. An AIR summarizing the interviewee's oral statement should be prepared by the monitoring special agent to supplement the DA Form 2802 (Polygraph Examination Report). This summary should omit any reference to the polygraph examination itself.

EXAMPLE
At 0900, 25 Mar 86, JONES was interviewed by SAs SMITH and WESSON. After being advised of his rights, JONES agreed to discuss the offense of murder, and executed the waiver portion of DA Form 3881. In an oral statement, JONES denied killing WILLIAMS and stated he was in Cleveland visiting his sick mother on 10 Mar 86, when WILLIAMS was shot.

This information will preclude JONES from inventing a better alibi should other investigative efforts demonstrate he was not in Cleveland, and it can be used at trial to impeach his credibility.

o. Refusal to undergo a polygraph examination

(1) Information relative to an individual's refusal to undergo a polygraph examination may only be recorded in the AAS or Internal USACIDC Memorandum for Record (MFR). The MFR will be attached to the USACRC, command, major subordinate command, and CID unit file copies of the final ROI. The MFR will not be listed as an exhibit to the ROI.

(2) The following information will be included on an MFR recording a refusal to undergo polygraph examination:

(a) ROI number.

(b) Name, grade, social security number, place and date of birth of the individual to whom the examination was offered.

(c) Date and place the polygraph examination was offered.

(d) Explanatory remarks concerning the circumstances under which the examination was offered, if appropriate.

(e) The individual's comments with reference to the refusal to take the examination, if appropriate.

(3) Information concerning a refusal to submit to a polygraph examination will not be disseminated outside USACIDC channels. This prohibits the

dissemination of polygraph refusal to SJA and unit/action commanders. Special agents may advise military police and civilian law enforcement officials of polygraph refusals in those instances in which the military police or civilian law enforcement agency is directly involved in the investigation in question.

p. Method of reporting results of polygraph examinations

(1) A Polygraph Examination Report will be utilized to report the results of polygraph examinations and will be an attached exhibit to the USACRC, USACIDC major subordinate command, action commander, and unit file copies of the final ROI, once polygraph quality control review reflecting a satisfactory examination has been accomplished.

(2) If a polygraph examination is conducted following submission of a final ROI, a supplemental ROI documenting the additional investigative activity will be prepared.

(3) When an individual has refused to submit to an examination but is interviewed by the polygraph examiner, the Polygraph Examination Report will be an attached exhibit only to the USACRC file copy of the final ROI. This restricted distribution is necessary to comply with the regulatory prohibition of reporting polygraph declinations to commanders.

q. Polygraph examination results may be recorded on a Polygraph Examination Report and a separate AAS. All AAS containing polygraph result information must be purged from the case file 90 days after the investigation is completed.

r. Information pertaining to the conduct or results of a polygraph examination may be made available, once polygraph quality control review has been accomplished, to action commanders, supporting SJAs, and local provost marshals. DA Form 2802 will be attached to all copies of the ROI once polygraph quality control review reflecting a satisfactory examination has been accomplished. A polygraph examination report disseminated outside USACIDC channels must bear the destruction statement identified in paragraph 2-5, AR 195-6. Any polygraph results that are made available prior to quality control review will be identified as tentative results that are subject to quality control review.

s. Special agents or their supervisors should, whenever possible, coordinate the facts and circumstances surrounding the need for the polygraph examination with the supporting polygraph examiner, prior to submitting the request for polygraph examination authorization to the approving authority.

t. Polygraph requests submitted via ACIRS CID E-Mail should be addressed to the USACRC E-Mail address. An information copy of all requests, regardless of

manner of transmission (facsimile, etc.) should be addressed to the appropriate USACIDC major subordinate commander.

u. Emergency requests during duty hours can be accomplished telephonically to USACRC, DSN 656-0457/0451. Emergency requests during non-duty hours can be accomplished telephonically to the USACRC Duty Technician, DSN 656-0397.

v. Requests submitted by other DoD elements to USACIDC units will be forwarded as specified in paragraphs g. and r. above.

w. E-Mail requests will be prepared in the format as shown in figure 5-5.

x. Questions regarding the propriety of a polygraph examination and requests for exception to the provisions of this regulation should be referred to the Commander, USACIDC, ATTN:
CICR-PD.

5-35
Intercept of wire and oral communications for law enforcement purposes

a. All USACIDC personnel, or persons acting on their behalf, will not engage in any intercept of wire, oral, or electronic communications without prior specific approval of the CG, USACIDC, or designee (i.e., DCO, Chief of Staff). See AR 190-53 for fuller definition of these terms. In general terms, the listening to or recording of conversations through the use of electronic, mechanical, or other devices without the prior consent of all parties to the conversation, constitutes a communication intercept for which prior authority must be obtained, with limited exceptions specified in AR 190-53. Requests to conduct communication intercept activities will be forwarded through the appropriate USACIDC major subordinate commander or, with the major subordinate commander's specific concurrence written into the request, directly to the Commander, USACIDC, ATTN: CIJA-ZA. Requests for communication intercept will only be submitted when based on the conditions cited in paragraph 1-4, AR 190-53, and will provide full particulars as outlined in paragraphs 2-1 or 2-2, or 2-5, AR 190-53. In exigent situations involving threats to human life, national security matters, or when time is of the essence, the request may be made telephonically to the HQUSACIDC JA, with follow-up written request.

b. Requests will be reviewed by HQUSACIDC JA to ensure administrative and legal sufficiency of the request. In the event the CG, USACIDC, supports the request, the request will be submitted to the Army General Counsel for further action.

c. See USACIDC Supplement 1 to AR 190-53 for additional guidance on interception of communications.

d. The use of telephone tracing equipment (e.g., lockout devices) may be authorized for legitimate law enforcement purposes to identify the origin of telephone calls to a subscriber user of a telephone. Specific guidance is found at chapter 4, AR 190-53 and 18 USC, section 3121 et seq. Coordination will be accomplished with the host installation communication-electronics office to determine their capability to support the operation and the potential cost. Any problems which surface as a result of this coordination will be resolved by the USACIDC major subordinate command C-E officer.

e. If available, and when its use will not create an unacceptable risk to sources or covert agents, technical listening equipment should always be used when executing a covert drug purchase; when, as part of an ongoing investigation, a registered source is undertaking any transaction with a suspect or subject; or when a covert agent is making a preplanned meeting with a suspect or subject. A mini-recorder should be used as a backup when a radio transmitter is used.

f. The use of pen registers is governed by chapter 3, AR 190-53, and 18 USC, section 3121 et seq.

5-36
National Crime Information Center (NCIC)

a. The NCIC is a nationwide computerized information system established as a service to all criminal justice agencies local, state, and federal. The goal of NCIC is to help the criminal justice community perform its duties by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information readily available to as many criminal justice agencies as possible. For NCIC purposes, "criminal justice information" is defined as "information collected by criminal justice agencies that is needed for the performance of their legally authorized, required function. This includes: wanted person information; stolen property information; criminal history information; information compiled in the course of investigation of crimes that are known or believed on reasonable grounds to have occurred, including information on identifiable individuals; and information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity."

(1) The Army NCIC terminals providing NCIC support to CID elements are primarily located with the installation Provost Marshal office. Data entry requirements are established by the FBI and the respective state wherein the NCIC terminal is located.

(2) The Army Crime Records Center (CRC) can enter persons into the NCIC wanted persons file provided USADIP has verified desertion status and maintains an active desertion entry in NCIC or if a USACIDC warrant for apprehension has been obtained. The CRC NCIC terminal operator can advise CID agents whether or not CRC can make an entry in the wanted persons file when the agent requests CRC assistance.

(3) The policy for NCIC participation is contained in AR 190-27 and, for Army deserters, in AR 190-9. Originating Agency Identifiers, (ORIs) have been established for all Army installations in CONUS.

(4) Agents are encouraged to request NCIC checks on subjects/suspects who have little active duty service time, who may have criminal histories which are not cataloged in the Defense Clearance and Investigations Index (DCII). NCIC queries related to name checks of a victim or witness are restricted based upon regulatory limitations imposed by the Department of Justice and the State of Virginia (who control and audit CRC's utilization of the NCIC system). If a name check of a victim/witness becomes a "critical element" to the investigation, then the Director, CRC, must have a written or e-mail request with sufficient details to justify the request, which will serve as justification during Federal and State audit processes. The CRC control technicians will not conduct a victim/witness name check without the approval of a CRC supervisor. If a telephonic request is approved, the requestor must follow it up with a written request.

(5) Lost or stolen U.S. Army weapons may be entered through Army NCIC terminals.

(6) Detailed instructions on the operation and use of the NCIC are prepared by the FBI and are available at each terminal site. Department of the Army policy encourages all military law enforcement activities to use NCIC facilities to the maximum extent. More than 50 U.S. Army installations operate communications terminals on NCIC over state telecommunications systems.

(7) The policy for NCIC participation is contained in AR 190-27 and, for Army deserters, in AR 190-9. Originating Agency Identifiers, (OAIs) have been established for all Army installations in CONUS. These OAIs are maintained by the Office of Army Law Enforcement (PEMP-O).

(8) Agents are encouraged to request NCIC checks on subjects/suspects who have little active duty service time, as well as spouses who may have criminal histories which are not cataloged in the Defense Clearance and Investigations Index (DCII).

b. Each USACIDC major subordinate command within CONUS will, in coordination with the agency responsible for the operation of the nearest terminal, establish procedures to ensure maximum utilization of the NCIC in the

conduct of USACIDC investigative operations. The USACIDC will ensure that entries are made into the NCIC files through USACRC, Army terminals located on the installation (when applicable), or through the terminal providing AOR NCIC support, if primary investigative responsibility rests with the USACIDC. Complete, accurate, and timely records are essential to ensure system integrity. Timely submission of information affords maximum protection to the law enforcement officer by providing up-to-date information. Although the use of NCIC is voluntary, delayed entry of records into the NCIC reduces the possibility of apprehending wanted persons, locating missing persons, and recovering stolen property. Upon receipt of identifying data, as described below, the CID element must submit the information to the supporting NCIC terminal by close of business (COB) the next working day, following assignment of the CID ROI number. Additionally, upon receipt of information verifying the recovery of property or the location of an individual entered in the NCIC system, the CID element must provide the information to the supporting NCIC terminal for removal of the record from the NCIC system, by close of business the next working day.

(1) Vehicle file: Enter stolen U.S. Government owned vehicles and aircraft whether stolen on or off-post. Enter privately- owned vehicles and aircraft when stolen from on-post locations. Privately owned vehicles stolen from off-post locations should be reported to local police and entered in NCIC as a result of the local civilian police NCIC activities. Removal of the entry will be in accordance with paragraph 5-36(b), upon the recovery or location of the vehicle.

(2) Gun file: Enter same as for vehicles. Stolen or lost U.S. Government weapons will be entered by local provost marshals in accordance with AR 190-11. Remove these records upon recovery in accordance with paragraph 5-36(b).

(3) Article file: Enter serial numbered stolen property, either government or privately owned, which is valued at $500 or more for each item. Serial numbered office equipment (adding machines, typewriters, etc.) will be entered regardless of value. Stolen serial numbered items may be entered regardless of value if the aggregate total is $5,000 or more. Serial numbered items may be entered regardless of value if there is a probability of interstate movement or the seriousness of the crime indicates that an entry should be made for investigative purposes. Recovered articles will be removed in accordance with paragraph 5-36(b). Re-entry of a purged article will begin a new retention cycle.

(4) Securities file: Enter serial numbered identifiable securities, which have been stolen, counterfeited, or lost. The term "securities" includes currency (bank notes, bills, etc.) bonds, debentures, notes, common or preferred stock certificates, traveler’s checks, money orders, and U.S. Treasury checks. Remove recovered securities in accordance with paragraph 5-36(b).

(5) Boat file: Enter stolen boats if they are registered/documented and there is a permanent serial number affixed. Remove recovered boats in accordance with paragraph 5-36(b).

(6) Missing persons file: Enter kidnapped individuals, runaways, persons who have disappeared for no apparent reason, and endangered persons, i.e., individuals who are known or believed to be with a person or persons who may harm them. The CID element must coordinate with their respective NCIC terminal coordinator to determine the individual State NCIC requirements for entry of individuals into the NCIC missing person files. Based on individual State requirements, additional documentation may be required. Remove located missing persons in accordance with paragraph 5-36(b).

(7) License plate file: Enter stolen license plates the same as for stolen vehicles. Remove recovered license plates in accordance with paragraph 5-36(b).

(8) Wanted persons file:

(a) CID "wants" on fugitive deserters. Only U.S. Army Deserter Information Point (USADIP), Personnel Control Facility, ATTN: ATZK-PMF-C, Building 1481, Fort Knox, KY 40121 can make fugitive deserter entries into NCIC; however, CRC can make an additional entry indicating the person is wanted by CID after USADIP has entered the individual as a deserter. This procedure is useful whenever a person who is wanted by CID is in a deserter status.

(b) CID "wants" supported by apprehension warrants. If a warrant for apprehension has been obtained in connection with a felony crime, the identity of the person wanted may be entered through any NCIC terminal; however, the preferred method is through USACRC. A signed warrant must be obtained from an authorized official based on probable cause to believe the wanted person committed a felony crime and a CID warrant number assigned (see paragraph 5-39) prior to entering the "want" into NCIC. This procedure may be used for any individual, whether or not in a deserter status. All CID supervisors must ensure that the seriousness of the crime warrants such action.

(c) Enter a temporary felony want when a subject's location is known and CID or MPI are ready to make an apprehension in conjunction with civilian police authorities. A temporary felony want record is automatically removed from file 48 hours after the entry. Accordingly, this procedure should be requested only when the CID/MPI apprehension is imminent. The temporary felony want should be used when the urgency of the circumstances require immediate action. The individual must be suspected of, or known to have, committed a felony offense. The suspect/subject's location should be known and there should be a strong probability of prompt and successful action to apprehend the person. Since one of the purposes of the temporary felony want is to protect police officers should

they unknowingly come in contact with fleeing felons, the NCIC terminal operator must be advised of any caution codes that should be included in the entry (e.g., armed and dangerous, escape risk, drug user, etc.) Additionally, temporary felony wants may be re-entered when necessary. The temporary felony want, as is the regular felony want, is used only when probable cause for the apprehension of an individual exists. Temporary felony want entries may be made through any Army NCIC terminal. The temporary felony want should be canceled when the suspect/subject has been apprehended.

c. All CID entries made through Army NCIC terminals will contain the entry "call CID (area code and phone number)" in the miscellaneous (MIS) field. The USACIDC element phone number will be used in this entry.

d. All NCIC entries for an apprehension authorization will include the authorization number in the miscellaneous number (MNV) field. Refer to paragraph 5-39 for instruction concerning the authorization number.

e. All USACIDC elements located outside of the United States will make entries into the NCIC concerning stolen privately owned weapons and stolen U.S. securities. Missing persons, temporary felony wants, and other stolen property (government weapons are reported by the PM), meeting the NCIC criteria above, will be entered when there is probability that the property or person(s) may re-enter the CONUS. This information will be provided by telephone, ACIRS CID E-Mail, or electrical message to the Director, USACIDC Crime Records Center by close of business (COB) the next working day, following assignment of the CID ROI number. Telephone requests will be confirmed by E-Mail or electrical message.

f. Care must be taken to avoid duplicate entries on the same property or individual, especially in those cases where investigative jurisdiction is assumed by another agency. In these cases, the USACIDC office conducting the investigation will coordinate with the other agency to ensure that duplicate entries are not entered.

g. Activities or agents that enter records into the NCIC are responsible for their accuracy, timeliness, and completeness. The FBI, as manager of the NCIC system, helps maintain the integrity of the system through: (1) automatic computer edit s which reject certain common types of errors in data; (2) automatic purging of records after they are in file a prescribed period of time; (3) quality control checks by FBI personnel; and (4) periodically furnishing lists of all records on file for validation by agencies that entered them.

h. Validation of all NCIC entries will be accomplished in accordance with schedules announced by the FBI and respective State in which the NCIC terminal that made the entry is located. All CID elements making NCIC entries will provide documentation to support the NCIC entry with the NCIC terminal

operator. This documentation will be filed by the NCIC terminal operator to support response to "hits" on the information and to provide validation information. The documentation should include the CID case number and any facts related to the entry. The CID element will participate in validation of their NCIC entries when requested by the Army NCIC terminal responsible for making the NCIC entry. The validation process includes a review of each active entry to ensure that the item is still active, that all information is current and accurate, and that the NCIC record contains all available data.

i. It is imperative that information entered into any NCIC file by CID be removed immediately when the wanted person is located or the article, security, vehicle, license plate, boat, or missing person is found.

j. All personnel using the NCIC system will ensure system integrity. Complete, accurate, and timely records are essential to ensure system integrity. Users also are encouraged to enter records in a timely manner to afford maximum protection to the law enforcement officer by providing up-to-date information. Although the use of NCIC is voluntary, delayed entry of records into the NCIC reduces the possibility of apprehending wanted persons, locating missing persons, and recovering stolen property. Promptness in modifying, locating, or clearing records in the system will help to keep the system free from stale information.

5-37
USACRC records checks

a. Request for USACRC records checks of suspects, subjects, and victims, are controlled by AR 195-2.

b. The USACRC routinely conducts record checks of suspects, subjects and victims listed in initial, status, and SSI (only) reports.

c. Any USACIDC special agent may make additional requests for USACRC record checks in furtherance of authorized Army law enforcement activities, when an immediate check is desired for information related to other than a suspect, subject, or victim (e.g., when a source is developed or a witness veracity is questionable). Requests for these additional record checks may be transmitted to the USACRC by letter, ACIRS CID E-Mail, electrical message, or telephone.

(1) Requests will include the following identification data when available:

(a) Last, first, and middle name

(b) Date of birth

(c) Place of birth

(d) Social security number

(e) Former service member

(2) When a request is submitted in writing or by message, the following actions will be taken:

(a) The request will include the sequence/ROI number with which the request is related.

(b) A copy of the request will be included in the case folder.

(c) If the reason for the request is not apparent, an explanation will be included in the AAS.

(3) When a request is submitted telephonically, the following actions will be taken:

(a) The requester will inform the USACRC of the sequence/ROI number with which the request is related.

(b) The requester will provide USACRC with their individual sequence number.

(c) The making of the request will be annotated in the AAS.

(d) If the reason for the request is not apparent, an explanation will be included in the AAS.

d. If a sequence number has not been assigned at the time of the request, the requester will provide the USACRC with the reason for request (e.g., criminal investigative activities).

e. A copy of the USACRC response will be included in the case folder or, if verbal, reflected in the AAS.

f. When making USACRC name checks on sources, the procedures in chapter 14 will be followed.

5-38
FBI records checks

a. A check of FBI records normally is not necessary unless there is a need to check the records of civilian police generated after the person in question

entered the military. A request for an FBI record check should be considered when investigating the most serious offenses or when it is particularly important to determine the total criminal history of an individual.

b. Request for FBI records checks will be accomplished by specifically requesting the USACRC to make the check as part of the USACRC name check request. In some cases, the existence of a recent National Agency Check (NAC) which includes an FBI name check will make a further FBI name check unnecessary.

5-39
FBI National Center for the Analysis of Violent Crime

a. The National Center for the Analysis of Violent Crime (NCAVC), Quantico, VA, is responsible for the Violent Criminal Apprehension Program (ViCAP), profile development, and crime scene analysis. All USACIDC field elements must coordinate with their supporting CID forensic science officer prior to submitting a ViCAP Crime Analysis Report (FD 676) or a request for a criminal personality profile evaluation.

b. The ViCAP is a nationwide data information program designed to collect, collate, and analyze all aspects of the investigation of violent crimes meeting certain FBI established criteria. The ViCAP is operated by the NCAVC and is for the use of all law enforcement agencies. Through analysis of data received, the ViCAP staff will determine if similar pattern characteristics exist in all crimes reported to ViCAP. The identification of similar patterns will be made by analyzing modus operandi, victimology, physical evidence, suspect description, and suspect behavior exhibited before, during, and after a crime. The overall goal of ViCAP is to provide law enforcement agencies reporting similar pattern violent crimes with the information necessary to initiate a coordinated multi-agency investigation to expedite the identification and apprehension of the offender responsible for the crime.

c. Whenever an investigation is determined to be reportable under ViCAP, an initial or status SSI report will be submitted (See paragraphs 7-10, 7-11, 7-12 and 7-13). The following categories of offenses are ViCAP reportable to the FBI:

(1) Solved or unsolved homicides or attempts, especially those that involve an abduction; are apparently random, motiveless, or sexually oriented; or are known or suspected to be part of a series.

(2) Missing person(s) where the circumstances indicate a strong possibility of foul play and the victim is still missing.

(3) Unidentified human remains, where the manner of death is known or suspected to be homicide.

d. All USACIDC elements will make entries into ViCAP utilizing the ViCAP Crime Analysis Report (FD 676). Forms will be provided by the FBI and can be requested by calling ViCAP at (703) 632-4254 or (800) 634-4097. Instructions for completion of Form 676 are included on the form. Assistance in completing the report is also available by calling ViCAP. All completed ViCAP forms will be forwarded directly to the ViCAP, FBI Academy, Quantico, VA 22135.

e. Cases where the offender has been arrested or identified should be submitted so unsolved cases in the ViCAP system can be linked to known offenders.

f. The NCAVC will only report database matches, or near matches.

g. Care must be taken to avoid submission of duplicate ViCAP reports on the same investigation, especially in those instances where investigative jurisdiction is assumed or shared with a domestic law enforcement agency. In those cases, the USACIDC unit conducting the investigation will coordinate with the other agency to ensure that duplicate reports are not submitted.

h. When a military member is a suspect, subject, or victim of any offense meeting ViCAP reporting criteria, and the investigation is controlled by a foreign law enforcement agency, the USACIDC will initiate a Collateral ROI (see paragraph 7-18) and submit ViCAP reports on the offense.

i. If a reporting USACIDC unit receives information that an investigation submitted to ViCAP has matching or similar patterns to reports submitted by other law enforcement agencies, direct coordination with those agencies is authorized.

j. Forensic science officers will review cases for potential analysis by the NCAVC. If the case meets the criteria for profiling, the forensic science officer will submit the entire profile package to the NCAVC. USACIDC units will submit criminal personality profiling case materials through their forensic science officers to the NCAVC.

5-40
Military

a. Search and Seizure Authorizations. A search warrant is an express permission to search and seize issued by a competent civilian authority. In the military, the term "search warrant" is actually an "authorization" to search a person, an area for specified property or evidence or for a specific person, and to

seize such property, evidence, or person. It may contain an order directing subordinate personnel to conduct a search in a specified manner. See Military Rule of Evidence (MRE) 315.

(1) A search and seizure authorization may be issued under this section for search of:

(a) Persons. The person of anyone subject to military law or the law of war, wherever found.

(b) Military property. Military property of the United States or of non-appropriated fund activities of an armed force of the United States, wherever located.

(c) Persons and property within military control. Persons or property situated on or in a military installation, encampment, vessel, aircraft, vehicle, or any other location under military control, wherever located.

(d) Nonmilitary property within a foreign country.

(2) A search and seizure authorization may be authorized by a commander, a military judge, or by a full assigned or part-time military magistrate.

(a) The basis for obtaining a search and seizure authorization is that probable cause which exists when there is a reasonable belief the person, property, or evidence sought is located in the place or on the person to be searched. A search and seizure may be based upon hearsay evidence in whole or in part. A determination of probable cause under this section shall be based upon any or all of the following:

1. Written or oral statements communicated to the authorizing official in person, via telephone, or by other appropriate means of communication.

2. Such information as may be known by the authorizing official that would not preclude the officer from acting in an impartial fashion.

(b) A search warrant or search authorization is not required under this section for a search based on probable cause (see MRE 315 (g)) when:

1. There is insufficient time to obtain authorization.

2. There is a lack of communication with search authority because of military operations.

3. A search of an operable vehicle is required.

4. The authorization is not required by the Constitution.

(c) Execution of the search authorization may be made by any person(s) listed in Military Rules of Evidence (MRE) 315(e).

(d) An inventory of any property seized in connection with a search and seizure authorization must be conducted. A copy of this inventory must be given to the person from whom the property is seized as soon as reasonably possible. This would normally be done using DA Form 4137.

(e) The person whose property is to be searched should be notified of the search, if possible. If not possible, a copy of the authorization will be left in a conspicuous location at the scene of the search.

(f) Specific guidelines for completing an affidavit, supporting a request for authorization to search and seize, are contained in AR 27-10. (See figure 5-7).

3. All oral requests will be summarized in writing within two working days following granting of the authorization. A copy of the summarized request will be provided to the authorizing official and attached as an exhibit to the final report. This will insure the basis for authorization is duly recorded and available for use as evidence during any subsequent judicial or administrative proceeding.

b. Apprehension authorization under RCM 302 (e)(2)(C) and (D). An apprehension authorization or an arrest warrant issued by competent civilian authority is required when the individual(s) to be apprehended is located in a private dwelling.

(1) AR 27-10 gives definitive guidance regarding the actual preparation of the apprehension authorization.

(2) Examples of a completed request and authorization to apprehend, are shown at figure 5-8.

(3) SJA Coordination. Close coordination with the supporting SJA must be maintained regarding the preparation of both search and seizure authorizations and warrants for apprehension. All CID special agents and their supervisors should always be mindful that only the authorizing official for the authorization/warrants needs to be convinced that probable cause exists to issue the authorization/warrant. The local SJA should not be used to sway the authorizing official one way or the other on a determination of probable cause. The information provided to the authorizing official should stand on its own and the CID special agent should be prepared at any later time to state or show exactly what information was provided to the authorizing official. The easiest way to accomplish this is to prepare a written affidavit or a memorandum of any oral conversations as soon as possible after the information is provided.

(4) In the event that an apprehension authorization is to be served off a military installation outside the CONUS, appropriate coordination with local civilian authorities must be made. Special agents should not execute an apprehension authorization off a military installation without the presence of civilian authorities in a foreign country.

(5) Apprehension authorizations and other arrest warrants obtained by the USACIDC will be numbered as follows: The first four digits will include the CID sequence numbers of the investigation for which the warrant was issued. The next two numbers are the year. The next three numbers are the CID unit number. Next, a dash and the number for the authorization pertaining to this investigation. For example, if only one authorization has been issued in an investigation, the last number would be -1. If, however, three authorizations had been issued for a particular investigation involving only one apprehension, authorization would be as follows: 0497 (CID sequence number) 93 (year) 122 (CID unit number) -1. An authorization number would look like this: 049793122-1.

(6) If the subject of an apprehension authorization is known to be "at large," it may be deemed appropriate to enter the authorization into the NCIC under the wanted persons file. Normally, this will be accomplished by sending a status report requesting that the entry be made. The following type of information is required to enter such persons into the NCIC: Full name; sex; race; place of birth; date of birth; SSN; height; weight; eye and hair color; warrant number; date; and offense(s). Other information may also be provided, if known, such as vehicle information. All of the information need not be sent if it is not available. Under extraordinary circumstances, the CID element may want to place such entries into NCIC through the use of the local MP or civilian police NCIC terminal. If this is done, coordination must be effected with the local NCIC operator for the correct information required to make the entry. In all cases, the authorization number should be placed in the NCIC miscellaneous number field (MNV).

c. Army Privacy Program (PCOMS). Army Privacy Communications, also called "back channel" messages, delivered to an intended recipient are record copies and become the recipient's property for control and disposition by AR 380-38. Access by CID agents for extraordinary purposes, such as investigative or judicial proceedings may be granted by the Director of the Army Staff (DAS) or higher DA authority as an alternative means to search warrants/authorizations or subpoenas.

(1) Agents will request a voluntary release from the recipient in all cases. If the recipient is not expected to comply voluntarily to a request (i.e., the recipient is the subject or suspect in the investigation), or if the agent is unsure of the recipient's inclination to comply with a request, and the time needed to obtain DAS permission, warrant, authorization, or subpoena would enable the recipient to destroy or hide the PCOMS, the agent will obtain DAS permission, warrant,

authorization, or subpoena prior to requesting voluntary release from the recipient.

(2) Requests for and justification for un-consented access shall be forwarded to CDR, USACIDC (CIJA-ZA), Fort Belvoir, VA 22060.

5-41
Federal

a. Complaints. In cases involving civilians who violate federal law in an investigation under the investigative purview of the USACIDC, consideration should be given to filing a criminal complaint against the individual(s). If the FBI does not assume responsibility for the matter under investigation, direct coordination with the appropriate U.S. attorney may be desirable. When such coordination is made and the investigation is presented to the U.S. attorney's office, he may elect to prosecute the matter. If the U.S. attorney who is briefed on the case deems it appropriate, he may elect to file a criminal complaint or criminal information. (See figure 5-9).

b. Arrest Warrants. Once a criminal complaint is prepared and sworn to by the appropriate official, the issuance of a federal arrest warrant may be deemed appropriate by the AUSA. If this course of action is deemed appropriate, the AUSA will assist in the preparation of the arrest warrant and the affidavit to support such a warrant. If the USACIDC special agent serves the arrest warrant on-post, the return portion of the arrest warrant must be completed upon service of the warrant. (See figure 5-10).

(1) Such arrest warrants may only be executed by the appropriate federal civilian authorities when the offender is located off the military reservation.

(2) On a military reservation, federal arrest warrants obtained by USACIDC special agents in connection with a USACIDC investigation may be executed by USACIDC special agents. If this course of action is taken, USACIDC special agents will immediately notify the nearest United States Marshals office and determine from that agency what the disposition of the offender should be.

c. Search warrants. In investigations involving the search of property not under military control, the issuance of a federal search warrant may be appropriate. If the USACIDC agent believes that a federal search warrant may be appropriate, the AUSA will be contacted and briefed on the investigation. If he deems a search warrant to be appropriate, based upon probable cause, the following types of search warrants may be obtained and served by USACIDC special agents:

(1) Search warrant on written affidavit. This type of search warrant is issued by a federal judge or United States magistrate, based upon probable cause, and supported by a written sworn affidavit. (See figure 5-11).

(2) Search warrant on oral testimony. This type of search warrant is issued by a federal judge or United States magistrate, based upon probable cause, and supported by a recording or oral testimony by the affiant. This type of warrant is authorized under very unusual circumstances during which a written affidavit cannot be prepared in a timely manner.

(3) If the search warrant is to be served off the Military reservation, the appropriate civilian police authority must accompany the CID special agent(s) executing the warrant. If the warrant is to be served on the military reservation, CID special agents or military police may execute the warrant as appropriate.

(4) On the rear portion of the search warrant is a return section. This section must be filled out when the warrant is executed and an inventory of the property is made.

d. Subpoenas

(1) Subpoena. During some USACIDC investigations it may become necessary to subpoena witnesses to appear before federal criminal justice proceedings. USACIDC special agents may request and serve a federal magistrate subpoena when a USACIDC investigation is involved.

(2) Subpoena Duces Tecum. Currently a Subpoena Duces Tecum may be used to obtain documents or information which may have value as evidence. This subpoena is obtained by providing the necessary information to the sup porting AUSA in order to verify the need for such a subpoena. This may be done orally or in writing, depending upon the desires of the AUSA. In all cases where federal subpoenas are obtained by USACIDC special agents, the return portion of the subpoena must be completed.

(3) DoD Inspector General (DoDIG) Subpoena

(a) The Inspector General Act of 1978, (5 USC, appendix 3 as amended by P.L. 97-252) provides subpoena power to aid the Inspectors General (IG) in their statutory mission to audit and investigate fraud, waste, and mismanagement. Section 6(a)(4) of the Act enables the IG to require, by subpoena, the production of all information, documents, reports, answers, records, accounts, papers, other data, and documentary evidence necessary in the performance of the functions assigned by the Act. The Act further specifies that the DoDIG is responsible for providing policy direction and guidance for audits and criminal investigations relating to fraud, and may request assistance, as needed, from other audit, inspection, and criminal investigative units of the DoD, including the military

departments (Sections (c)(2), (3), (5), and (8), 5 USC, appendix 3). The DoDIG relies on the military criminal investigative organizations to bring to his attention certain criminal investigations that merit his personal attention. Many of these investigations need additional documents outside a court-martial proceeding. When these situations arise, the military criminal investigative organizations are encouraged by the DoDIG to inform him of these investigations via a "Request for Subpoena(s)." Once received, the DoDIG will make an independent determination of whether the investigation falls within the scope of his statutory authority and, if so, will decide whether a subpoena is appropriate. If a subpoena is issued, the DoDIG will request that the military criminal investigative organization continue to investigate on his behalf, and when doing so, the restrictions of the Posse Comitatus Act (18 USC 1385) do not apply. (5 USC , appendix 3, section 8(g)). As the investigation proceeds, the DoDIG requires updates to keep him informed of the investigation. It should be noted that the DoDIG has issued subpoenas in support of administrative proceedings and audit functions, in addition to assisting in ongoing criminal investigations. The DoDIG subpoena has been proven to be a valuable investigative tool, especially since it avoids the problems created by Rule 6(e), Federal Rules of Criminal Procedure.

(b) Information obtained under a DoDIG subpoena is not subject to the secrecy requirements of Rule 6(e), Federal Rules of Criminal Procedure, and may also be used in support of civil litigation and administrative remedies. Thus, the DoDIG subpoena is preferable in some respects to federal grand jury subpoena; however, unlike the grand jury subpoena, it cannot compel testimony.

(c) Prior to requesting a DoDIG subpoena, the case agents will perform the following:

1. Solicit consent of the person(s) or organization(s) concerned, if investigation is overt, to voluntarily relinquish needed documents (Note: In the case of financial records, the detailed consent provisions of paragraph 5-42 concerning the Right of Financial Privacy Act must be strictly followed).

2. Coordinate with supporting SJA and/or local AUSA to determine if the needed documents can be obtained under some other auspices, such as a contract clause requiring records be made available for government review.

(d) If a DoDIG subpoena is deemed the best way to obtain needed documents, the case agent will prepare and submit to the major subordinate command JA a DoDIG subpoena packet, consisting of a memorandum request, subpoena cover letter, and a certificate of compliance, as well as a Privacy Act notice. (Additional documentation is required if financial records are sought. See paragraph 5-42). Generally the Right to Financial Privacy Act (RFPA) applies if the subpoena recipient is a bank, savings and loan, credit union, or credit card issuer and the account holder is an individual or partnership of five or fewer

people (See 12 USC 3401 et. seq.) The request for Inspector General Subpoena will detail the information outlined within figure 5-33.

(e) Upon receipt of the approved subpoena, the field element will serve a copy of the subpoena personally or via registered mail, and notify CDR, USACIDC, ATTN: CIJA-ZA via ACIRS E-Mail or electrical message. The certificate of return of service located on the reverse side of the original subpoena will be completed and forwarded to CDR, USACIDC, ATTN: CIJA-ZA for transmittal to the DoDIG. Decisions not to serve an approved subpoena must be immediately reported to CDR, USACIDC, ATTN: CIJA-ZA.

(f) If a subpoena target fails to comply, or complies only partially, immediate notification will be made to CDR, USACIDC, ATTN: CIJA-ZA, who will provide further instructions.

(g) Originals or certified copies of documents obtained should be safeguarded, although in most instances they will not be classified as physical evidence as defined in AR 195-5. At a minimum, an inventory of all documents will be prepared. Access to these documents will be limited to case agents(s) and supervisors(s). The documents will be stored under lock and key.

(h) The DoDIG requires periodic updates on cases involving the use of DoDIG subpoenas. Unless otherwise instructed by the HQUSACIDC, Category II/III monitorship updates and/or routine status reports provided to HQUSACIDC will satisfy the periodic update requirement. The final report of investigation will be forwarded to the DCSOPS, USACIDC, ATTN: CIOP-COP, to facilitate closure of DoDIG subpoena request files.

(4) Federal grand jury subpoenas

(a) Certain investigations will be conducted under federal grand jury proceedings. In these instances, the case agent is typically appointed as an agent of the grand jury and the investigation is controlled and directed by the impaneled grand jury.

(b) The grand jury is empowered to issue subpoenas to obtain testimony, documents, etc., in furtherance of its investigations, and may direct USACIDC agents to serve these subpoenas and maintain custody of materials acquired.

(c) As stated previously, a DoDIG subpoena is preferred over a grand jury subpoena, because grand jury proceedings fall under the purview of Rule 6(e), Federal Rules of Criminal Procedures, which imposes strict secrecy on information obtained. Additionally, information obtained under a grand jury investigation may not be used to support civil litigation or administrative remedies. However, the grand jury subpoena has as an advantage, the ability to compel testimony.

e. Federal Summons. Not all USACIDC investigations involving civilians as subjects will lead to a criminal trial. In this same light, not all civilian subjects who are tried in U.S. Federal courts are actually arrested. In many cases, after coordination with the U.S. attorney, it may be deemed appropriate to issue a summons in lieu of requesting an arrest warrant. USACIDC special agents may request and serve a federal summons when a USACIDC investigation is involved. As in the case of other federal processes, the return portion of the summons must be completed when the summons is served. (See figure 5-15). As with federal subpoenas, the U.S. Marshal's office will provide assistance as appropriate if it is believed that difficulty ma y be encountered in serving the summons off of a military installation.

f. United State District Court Violation Notice (DD Form 1805). If, for any reason, it is not possible to prosecute a civilian offender in federal district court for a crime committed on a military reservation, consideration should be given t o issuing a DD Form 1805 to the offender. Only misdemeanor crimes and petty offenses can be heard by the U.S. magistrate. An example might be a civilian government employee who steals approximately $1,000 worth of government property and the U.S. attorney will not prosecute. In this instance, consideration should be given to charging the employee with 18 USC, 641 (theft of government property), a lesser included offense. If convicted of the offense, the employee will have a criminal record and may have his employment terminated based upon his federal conviction. While not the most desirable manner in which to handle such a case, referring the matter to the U.S. magistrate as a misdemeanor is better than taking no judicial action at all. Any decision to utilize the DD Form 1805 under this section should be fully coordinated with the special assistant U.S. attorney (SJA) who handles the local magistrate court prosecutions. AR 190-29 (Misdemeanors and Uniform Violation Notices Referred to US Magistrate or District Courts) outlines the specific guidance for completing this form.

5-42
Other civilian warrants

From time to time during USACIDC investigations, it may become necessary to obtain search and arrest warrants from local civilian officials, both inside and outside CONUS. Any USACIDC special agent may seek such warrant s if deemed appropriate by a USACIDC supervisor and local civil authorities; however, only local police authorities may execute such warrants. Special agents are limited to assisting in identifying persons subject to military law and the identification of U.S. Government property.

5-43
Financial records of private persons

a. General. The Right to Financial Privacy Act of 1978, as implemented by AR 190-6, establishes well defined procedures for obtaining the financial records of private persons within the United States, its territories, and possessions. It is mandatory under federal law that the procedures described in subparagraphs c through j below be followed. The Financial Privacy Act does not pertain to financial records of partnerships of more than five persons, corporations, associations, trusts, or financial records of other legal entities. (These financial records may be obtained in the normal manner by request, subpoena, or search warrant). Neither does the Financial Privacy Act restrict the obtaining of the pay records of military personnel or Department of Defense employees. The following definitions, although not the only ones addressed in the statute, are of particular importance to CID special agents:

(1) A "person" is defined as an individual or a partnership of five or fewer people.

(2) A financial institution is any office of a bank, savings bank, industrial loan company, trust company, savings and loan association, homestead association (including cooperative banks), credit union, and consumer finance institution. Included are those offices located in any state or territory of the United States, or in the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands. Also included are credit card issuers, including businesses which issue credit cards as a means of promoting sales (such as department stores and gasoline companies). In the case of these businesses, however, the Financial Privacy Act applies only to transactions made through the use of the credit card. Cash transactions and credit purchases not made with the credit card are not covered.

(3) A financial record is defined as an original record, its copy, or information known to have been derived from the original record held by a financial institution, pertaining to a customer’s relationship with the financial institution.

b. Basic identifying account data. Basic identifying account data, including customer's name, address, account number, and type of account, may be requested from a financial institution without complying with the customer notice, challenge, o r transfer procedures described elsewhere in this paragraph. (See figure 5-20).

c. Initiation of requests. All CID supervisors of field grade rank are authorized to initiate requests for access to financial records.

d. Customer consent. If access to financial records is gained through the consent of the person to whom the records pertain, the consent must be in writing, dated, and signed by the customer. The consent document must identify the records being disclosed, specify the purpose for disclosure, and the agency

to which the records are to be released; state that the consent may be withdrawn at any time before disclosure; and authorize the disclosure for a period not to exceed three months. (See figure 5-21). Additionally, the person must be provided a "Statement of Customer Rights Under the Right to Financial Privacy Act" (see figure 5-22). A copy of the signed consent form will be filed in the case file.

e. Search warrants. Access to financial records may be obtained through use of a search warrant issued under Rule 41 of the Federal Rules of Criminal Procedure. A copy of the search warrant and the following notice must be mailed to the person's last known address within 90 days of the service of the warrant:

"Records or information concerning your transactions held by the financial institution named in the attached search warrant were obtained by this agency on (date) for the following purposes: (state purpose). You may have rights under the Right to Financial Privacy Act of 1978."

f. DoDIG and judicial subpoenas. Access to a person's financial records may be accomplished through a DoDIG subpoena obtained in accordance with paragraph 5-40d(3) or a judicial subpoena obtained from a federal district or military court, as appropriate. Before acquiring the records, the individual must be given an opportunity to contest the subpoena. This is accomplished by serving the individual by mail or in person with a copy of the subpoena and the Customer Notice (see figure 5-23). This service must be accomplished on or before the date the subpoena is served on the financial institution. A Statement of Customer's Rights (see figure 5- 22), a blank copy of a Customer's Motion to Challenge Government's Access to Financial Record s (see figure 5-24), a Customer's Sworn Statement for Filing a Challenge (see figure 5-25), and an instruction sheet informing the customer how to complete the motion form and sworn statement (see figure 5-29), will be provided the individual at the same time. The customer shall have 10 days if service of these papers is in person or 14 days if service is by mail to file a challenge with the appropriate federal court. The case agent or major subordinate command JA should check with the clerk of the court to determine if a challenge has been filed. Access to financial records cannot be obtained until the time to file a challenge has expired; or, if a challenge is filed, it has been acted upon by the proper court. Note: grand jury subpoenas may also be used to obtain financial records.

g. Formal request to a financial institution. Access to financial records by means of a formal written request to the financial institution may only be obtained if the customer has previously declined consent to disclosure or if seeking consent would compromise or harmfully delay the investigation. (See figure 5-26). At the same time or prior to the time the request is issued to the financial institution, a Notice of Formal Written Request (see figure 5-27), together with a copy of the request to the financial institution, a blank copy of a Customer's Motion to Challenge Government's Access to Financial Records, and a Customer's Sworn

Statement for Filing a Challenge will be served upon or mailed to the person whose financial record s are being sought. That person will then have 10 days, if served personally, or 14 days, if served by mail, to file in the proper federal court a challenge to the request for access. The case agent or major subordinate command JA should check with t he clerk of the court to determine if a challenge has been filed. Access may not be obtained until the time to file a challenge has expired; or, if a challenge is filed, it has been acted upon by the court.

h. Certificate of compliance. The CID supervisor initiating the request for access to financial records shall provide to the financial institution prior to, or at the time access is actually obtained, a certificate indicating compliance with all requirements of the Right to Financial Privacy Act of 1978. (See figure 5-28).

i. Emergency access. Emergency access to financial records may be obtained if delay incidental to the normal notice procedures would create an imminent danger of physical injury, serious property damage, or flight to avoid prosecution. In the se situations, a certificate of compliance will be provided the financial institution at the time access is obtained. Within five days of that time, the requesting official will file with the proper federal district court a sworn statement setting forth the grounds for the emergency access. Additionally, the customer will be served with, either in person or by registered or certified mail, return receipt requested, a copy of the request to the financial institution and the following notice:

"Records concerning your transactions held by the financial institution named in the attached request were obtained by (name or agency) under the Right to Financial Privacy Act of 1978 on (date) for the following purposes: (state the nature of the law enforcement inquiry). Emergency access to such records was obtained on the grounds that: (state grounds)."

j. Transfer of information. If financial information obtained pursuant to the Financial Privacy Act is transferred to another federal agency outside of the Department of Defense (including the FBI or a U.S. attorney), the transferring CID element must first certify in writing that there is reason to believe that the records are relevant to a law enforcement investigation within the jurisdiction of the receiving agency. Justification to support this certification may be requested from the receiving agency and should be included in the certificate. A copy of the certificate will be included in the case file with the records. Additionally, a copy of the certificate and the following notice must be served upon or mailed to the person to whom the records pertain within 14 days of the transfer:

"Copies of, or information contained in, your financial records lawfully in the possession of the Department of the Army have been furnished to (name of receiving agency) pursuant to the Right to Financial Privacy Act of 1978 for (state the purpose). If you believe this transfer has not been made to further a

legitimate law enforcement inquiry, you may have legal rights under the Financial Privacy Act of 1978 or the Privacy Act of 1974."

k. Delay in customer notification. When seeking or transferring financial records by following procedures outlined in subparagraphs e, f, g, i, and j above, delays in the required customer notifications required by subparagraphs d through f, h, and i above may be granted by the proper court if such notification would result in endangering the life or safety of any person, flight to avoid prosecution, intimidation of witnesses, or otherwise seriously jeopardize the investigation or proceeding. If the court grants the delay, it will also issue an order prohibiting the financial institution concerned from revealing that financial information has been requested or obtained. In the case of formal written request to a financial institution, administrative or judicial subpoena, emergency access, or release of information to other federal agencies, a court may grant delay for successive periods of 90 days. In the case of a search warrant, an initial delay of 180 days with successive de lays of 90 days may be granted. Upon the final expiration of any delay period(s), the following must be provided the customer in lieu of the notice normally required:

(1) In the case of a search warrant, mail a copy of the search warrant and the following notice:

"Records or information concerning your transactions held by the financial institution named in the attached search warrant were obtained by this agency on (date). Notification was delayed beyond the statutory 90-day delay period pursuant to a determination by the court that such notice would seriously jeopardize an investigation concerning (state with reasonable detail). You may have rights under the Right to Financial Privacy Act of 1978."

(2) In the case of a formal written request to a financial institution, serve personally upon or mail to the customer a copy of the request and the following notice:

"Records or information concerning your transactions which are held by the financial institution named in the attached process or request were supplied to or requested by the government authority named in the process or request on (date). Notification was withheld pursuant to a determination by the (title of the court) under the Right to Financial Privacy Act of 1978 that such notice might (state reason). The purpose of the investigation was (state purpose with reasonable detail).

(3) In the case of emergency access, serve personally or mail to the customer a copy of the request and the notice described in subparagraph "i" above.

(4) In the case of transfer of the financial records to another federal agency outside DoD, the transferring CID element will serve personally or mail to the

customer the notice required in subparagraph "j" above. If the CID element w as also responsible for obtaining the court order authorizing the delay in notification, the notice required in subparagraph "k(2)" will also be personally served upon or mailed to the customer.

l. Marking of financial records and reports of investigation. Financial records and derivative information obtained pursuant to the Right to Financial Privacy Act will be marked as follows:

"This record was obtained pursuant to the Right to Financial Privacy Act of 1978, 12 USC 3401, et seq., and may not be transferred to another federal agency or department outside DoD without prior compliance with the transferring requirements of 12 USC 3412."

Reports of investigation or any other correspondence which contain information obtained under the Right to Financial Act will have the following warning stamped or typed on the first page or cover of the document:

"Some of the information contained herein (cite specific paragraphs) is financial record information which was obtained pursuant to the Right to Financial Act of 1978, 12 USC 3401 et seq. This information may not be released to another federal agency or department outside the DoD without compliance with the specific requirements of 12 USC 3412 and AR 190-6.

m. Overseas areas. Financial records maintained by military contract banking facilities in overseas areas may be obtained without the person's consent through use of a military search authorization obtained under the UCMJ and AR 27-10. Financial records from other financial institutions must be obtained in accordance with the laws of the nation in which the institution is located.

n. Reporting requirements. All USACIDC elements will provide the required data (see AR 190-6) directly to the supporting installation provost marshal on a quarterly basis.

5-44
Obtaining information from the U.S. Customs Service on monetary transactions under the Bank Secrecy Act

The U.S. Customs Service is the central repository for reports filed pursuant to the Financial Record keeping and Currency and Foreign Transactions Reporting Act of 1970 (P.L. 91-508). A report analysis unit receives, analyzes and maintains IRS Form 4789 (Currency Transaction Report), Customs Form 4790 (Report of International Transportation of Currency or Monetary Instrument Report), and Treasury Form 90-22.1 (Foreign Bank Account Report). Selected information is entered into a computer database for rapid retrieval and analysis.

In August 1985, USACIDC was approved for access to these records. The following procedures identify the manner in which the requested information may be obtained:

a. A written request from the SAC or district/field office commander must be made to the local Customs special agent-in-charge. A standard format letter may be used but must include:

(1) Specific name(s) to be checked;

(2) Any identifying data available;

(3) What violations of law are being investigated; and,

(4) A summary of the investigation.

b. Upon submission of the written request for Bank Secrecy Act (BSA) information, the local U.S. Customs special agent-in-charge is authorized to immediately disseminate available BSA information. Further dissemination of BSA data outside of the requesting agency must not occur without the specific approval of the Secretary of the Treasury or his authorized delegate.

c. Request made by CID offices OCONUS should be forwarded to the local Customs attaché.

d. Copies of BSA forms required as evidence for court presentation must be made in writing by the CG, USACIDC to the following address:

U.S. Customs Service
Chief, Currency Programs Section
1301 Constitution Avenue, N.W.
Washington, DC 20229

5-45
General

This section provides guidance and procedures to be followed by USACIDC personnel when supporting U.S. (or other Justice Department) attorneys in the conduct of Federal grand jury investigations. It also establishes procedures to be followed in handling and storing grand jury material and incorporating such material into CID reports of investigation.

5-46
Grand jury functions

a. The protection provided by the grand jury system are based upon the guarantees of the Fifth Amendment to the United States Constitution. These protections, as amplified by Rule 7, Federal Rules of Criminal Procedure (FRCP), require that offenses, which may be punishable by death, must be prosecuted by grand jury indictment; offenses which may be punishable by confinement for more than one year must also be prosecuted by grand jury indictment unless indictment is waived by the accused. Although not required, offenses other than these may also be prosecuted by indictment. Grand jury proceedings as such exist only in a civilian court setting and do not apply to the military judicial system. Within the military, a hearing under Article 32, UCMJ, serves essentially the same purpose as does the grand jury.

b. Because the grand jury process is intended to protect the individual rights of citizens, all grand jury hearings, deliberations, and votes are done in secrecy [Rule 6(d) and (e), FRCP]. These rules of secrecy extend to all "matters occurring before the grand jury" and bind not only the jurors themselves, but also government attorneys presenting the case and all administrative and investigative personnel assisting the attorney in presentation of the case. The secrecy restrictions may be lifted only by order of a federal court. There are normally no criminal sanctions for violation of the rules of secrecy, but individuals who do violate them may be held in contempt of court. It should be noted that secrecy rules are not applicable to witnesses before a grand jury insofar as their own testimony is concerned. Witnesses may, however, be requested not to reveal their testimony.

5-47
Matters occurring before the grand jury

a. No precise definition of "matters occurring before the grand jury" is contained either in statutes or the FRCP; its meaning has been developed through case law. Because of this, there may be some variation in definitions among the U.S. circuit courts and the U.S. district courts. The advice of the U.S. (or other Justice Department) attorney should be sought on any questionable matters. Generally, however, anything which will reveal what transpired during grand jury proceedings, oral testimony given before the grand jury, grand jury deliberations and votes, targets of the grand jury inquiry, identities of the jurors, grand jury subpoenas not a matter of public record, materials which would reveal the strategy or direction of the grand jury investigation, and the nature of evidence produced before the grand jury are classed as matters occurring before the grand jury. Also included are written transcripts or memoranda of testimony given by witnesses in front of the grand jury. Although, as a general rule, statements made outside the grand jury room do not constitute "matters occurring before the grand jury," the U.S. Attorneys' Manual suggests that, if a witness is interviewed

after appearing before a grand jury and relates what was said before the grand jury, any record of that interview is considered to be grand jury material.

b. Information and material not normally considered to be grand jury material includes statements and evidence gathered through the normal investigative process prior to the commencement of hearings of a case by the grand jury, even though this material may eventually be presented to the grand jury. Also not usually included are documents subpoenaed by the grand jury, if the documents were created for purposes other than grand jury use (e g., records prepared in the normal course of business) and their release subsequent to being subpoenaed will not reveal the direction or strategy of the grand jury investigation. In the case of subpoenaed records, however, it must be remembered that these remain the property of the party from whom subpoenaed, and may be released to third parties only with permission of the owner or by court order. This restriction applies to copies of and verbatim extracts from such records. Disclosure of subpoenaed material may also be restricted by other federal law such as the Right to Financial Privacy Act of 1978 or the Tax Reform Act of 1976.

5-48
Use of grand jury materials in civil proceedings

a. The government is precluded from using grand jury materials, not a matter of public record, in civil proceedings except by court order upon a showing by the government of a particularized need. It is for this reason that the use of means other than a grand jury subpoena (e. g., search warrant, DoDIG subpoena, see paragraph 5-40) is strongly encouraged when gathering evidence and expected testimony. Similarly, the preparation of an interim report of investigation (see paragraph 7-15) prior to beginning presentation of a case to a grand jury will document what evidence has been collected independently of the grand jury process. It is also for this reason that at least two special agents be totally knowledgeable of a case up until the time grand jury investigation begins. Thereafter, and in this manner, one will be able to assist the grand jury investigation, and, if necessary, the other able to pursue an untainted, parallel, independent investigation for purposes of possible civil recovery.

b. It is possible to make grand jury material a matter of public record and thus free it from the secrecy requirements of Rule 6(e) by having the material included by the U.S. (or other Justice Department) attorney in various documents such a s the sentencing memorandum [a sentencing memorandum is prepared by the U.S. (or other Justice Department) attorney following conviction and used by the court in arriving at an appropriate sentence], and other government pleadings so long as they are a matter of public record and not under seal. Such pleadings may include information; indictments; complaints; and affidavits in support of searches, arrests, and electronic surveillance. This approach should be

considered and appropriate recommendations made to the U.S. (or other Justice Department) attorney when grand jury material which may be of use to the government in civil recoveries was not presented at a criminal trial.

5-49
Access list

a. As a general rule, only the grand jurors, attorneys for the government, and administrative and investigative personnel necessary to support the grand jury process may have access to grand jury materials. The government attorney presenting the case to the grand jury is responsible for determining what individuals will have access to grand jury material, for preparing and updating an access list naming these individuals, and advising the court of who is on the access list. Persons having access to grand jury materials may only utilize that material for purposes of assisting the government attorney in the performance of his duties to enforce federal criminal law.

b. The Assistant U.S. (or other Justice Department) attorney presenting a case to a grand jury should be requested to place the following persons on the grand jury access list (this should be accomplished prior to these persons having actual access):

(1) Special agents assigned to assist the grand jury investigation.

(2) A limited number of CID supervisory personnel as needed, who must have access to properly complete the investigation and perform their supervisory functions.

(3) Evidence custodian, if necessary, to secure any grand jury material as evidence.

(4) Administrative personnel such as typists who must have access for preparation and/or processing of documents and records.

(5) Crime Records Center personnel who will be responsible for long-term storage of any summaries or extracts of grand jury materials in the custody of the USACIDC. (See paragraph 5-52c).

5-50
Security and accountability of grand jury materials

a. Grand jury materials, as well as any documents or records subpoenaed by the grand jury, will be stored in separate, secure, and locked rooms or storage containers. The material should be conspicuously marked in red as 'Grand Jury

Material' to allow their ready identification as such. Only those persons on the grand jury access list will be authorized entrance to or possession of keys or combinations to the storage room or containers.

b. A complete inventory must be prepared of all written grand jury material and all material subpoenaed by the grand jury. The inventory will list each document by name, date if any, the number of pages, and, if needed, a brief description of the document sufficient to allow its ready identification. This inventory will be retained with the grand jury materials, since the inventory itself may be indicative of the thrust of the grand jury investigation or the targets of the investigation.

c. There is no requirement to process subpoenaed material as evidence until a determination is made that the material does, in fact, have evidentiary value. Once such a determination is made, the material will be processed and accounted for in accordance with AR 195-5. When placed in the evidence room, the material will be in separate sealed packages or placed in locked containers within the evidence room to preclude accidental access by persons accompanying the evidence custodian. Grand jury material will be exempt from quarterly inventories except in bulk form; e. g., one sealed box containing grand jury material.

5-51
Grand jury subpoenas

See paragraph 5-40d(4) for procedures for obtaining and serving grand jury subpoenas.

5-52
Transmission of grand jury material

Grand jury material or information extracted there from, which is not a matter of public record, will not be transmitted by electrical message or by fax. Such material will be hand carried or mailed by registered mail, return receipt requested. If mailed, the material will be placed inside a sealed envelope and that envelope marked "Grand Jury Material. To be opened by authorized personnel only." That envelope will then be placed within a second, unmarked envelope. Envelopes or packages containing grand jury material will not be opened by persons not authorized access thereto.

5-53
Grand jury material in reports of investigation

a. No grand jury material will be incorporated into initial, status or interim reports of investigation.

b. Any information or evidence, originally classed as grand jury material, which is presented at a trial of the matter under investigation, is no longer covered by the secrecy requirements of Rule 6(e), FRCP. Such information or documents ma y, as necessary, be included in final or supplemental reports of investigation. When a final report of investigation is prepared prior to trial, and the grand jury material presented at trial adds significantly to the understanding and substantiation of the case, a supplemental ROI will be prepared, explaining the new evidence, and including any documentation as exhibits. When including such documents, care must be taken to insure that all information contained in the document was, in fact, introduced in open court. If not, a copy of the document, with the unrevealed portions excised, will be included as an exhibit.

c. Grand jury material which is not a matter of public record, but which is required for listing individuals as subjects or for a complete understanding of the investigation will be incorporated into final or supplemental reports of investigation as follows. No original materials or duplicate copies thereof will be included in a report of investigation. Summaries of and, if necessary (as a narrow exception to the prohibitions of the preceding sentence), limited extracts from the material will be prepared and placed inside a sealed and taped envelope, or, if particularly voluminous, inside sealed cardboard cartons. The envelopes/container(s) will be plainly marked "Grand Jury Material" together with the report of investigation number. An inventory of the documents, prepared in accordance with paragraph 5-49b, will be included. An entry will be made in the attached exhibits section of the "original copy only" of the report of investigation as follows: "Grand Jury Material Attached." Grand jury material will be attached only to the original copy of a report of investigation. Reports of investigation forwarding grand jury material to the CRC will be sent by registered mail, return receipt requested.

5-54
Storage at Crime Records Center

a. Summaries and extracts of grand jury materials received by the Crime Records Center will be provided security comparable to that described in paragraph 5-49a above. The Director, Crime Records Center, or his deputy will designate one or more persons as the custodian of these materials and only those custodians shall have access thereto. The name of this custodian(s) will be included on the USACIDC access list when it is being prepared for submission to the Assistant U.S. or other Just ice Department attorney conducting a grand jury investigation.

b. Grand jury material on file at the Crime Records Center will be released or disposed of only as authorized by a U.S. or other Justice Department attorney, a court of competent jurisdiction or in accordance with Federal law.

5-55
Disposition of grand jury material

The Department of Justice, through its various U.S. attorneys, is responsible for permanent storage of grand jury materials. When no longer required for the grand jury investigation, prosecution, or other immediate needs of the U.S. (or other Department of Justice) attorney, grand jury materials in the possession of USACIDC units will be returned to the appropriate U.S. attorney. Original materials subpoenaed for a grand jury investigation will also be returned to the U.S. attorney, or after coordinating with and obtaining the approval of the U.S. attorney, returned to the rightful owner.

5-56
Media relations

All USACIDC field elements will fully support DoD and DA policy to inform the public of the Army's unclassified activities, except in those circumstances where such information is restricted from disclosure. Field elements will honor requests for information from public affairs officers (PAO) pursuant to requests originating from news media organizations, to the extent authorized by existing laws and DoD/DA regulations. Field elements will refer direct calls (or contact) from news media representatives to supported public affairs officers, without comment. Field elements are prohibited from releasing any USACIDC case related information (to include any oral reiteration of case information or supposition) directly to any news media representative.

5-57
Public Website Administration

a. Publicly accessible websites are authorized to be created, subject to the following approval procedures:

(1) All information placed on the World Wide Web (WWW) is required to be cleared for public release in the same manner as if it were released through any other medium, in accordance with AR 360-1, The Army Public Affairs Program. Requests for authorization to publish websites will be sent through command channels to the Chief, Public Affairs Office (PAO), HQUSACIDC, prior to uploading for public access. The request will include a complete copy of the proposed website either in printed or electronic format.

(2) Websites must conform to the provisions of reference 1d and to Department of the Army policy.

(3) Each element maintaining a website will institute procedures to ensure the information provided remains current.

(4) Every website will include the name and e-mail address of the individual responsible for the website content and will contain the date of the last modification.

(5) Official CID publicly accessible websites will not be housed on privately-owned servers. Homepages will be maintained on the installation's Director of Information Management (DOIM) web server. A CID unit with proper DOIM coordination and approval, may maintain its own stand-alone web server. At no time will a USACIDC website share the same local area network as the Automated Criminal Investigative Reporting System (ACIRS) or with any other networked office automation database computer.

(6) Personal websites created and/or owned by any employee of the USACIDC will not reference any USACIDC operations, procedures or policy unless the content is approved for release by the Chief, PAO, HQUSACIDC, and the Office of the Staff Judge Advocate, HQUSACIDC.

(7) Each CID element's website will contain a link to the HQUSACIDC public website.

b. The following are not authorized for publication on publicly accessible websites:

(1) Statistical Data.

(2) Cites or quotes taken directly from any USACIDC, Army or DOD regulation, standard operating procedures, policy memoranda, or any internal document not normally made available to the public.

(3) Personal information on the personnel assigned to the USACIDC element. Names of key personnel may be published as well as the normally published office telephone number. The individual's title will be used in lieu of their rank/pay grade.

(4) Operational security type information such as unit manning levels, modified table of organizational equipment, mission functions, or listings of unit personnel by their position.

5-58
Public Appearances and Presentations by USACIDC Personnel

a. Annually, USACIDC agents and examiners train in various venues, i.e., FBI National Academy, Canadian Police College, American Academy of Forensic Sciences and the American Polygraph Association. This interaction with other law enforcement personnel not only provides USACIDC personnel with quality professional development training, but also exposes other agencies to USACIDC. Presentation of investigative materials is often required for coursework or for advancement within the professional community. USACIDC active contribution displays the quality of USACIDC investigative work and the proficiency of USACIDC agents.

b. The information presented in these forums must comply with the Joint Ethics Regulation procedures for teaching, speaking and writing. Public speaking, writing or teaching concerning national security matters, USACIDC operational matters, forensics or policies will not be presented without prior approval from HQ, USACIDC.

c. Any requests for USACIDC personnel to speak or present topics regarding USACIDC investigations, forensic work, operations or policies at events not sponsored by military/federal government organizations must be reported to the Chief, Public Affairs Office, HQUSACIDC, prior to acceptance of the invitation. Public Affairs Office will coordinate the invitation with the Current Operations, DCSOPS and the Ethics Counselor, Office of the Staff Judge Advocate, HQUSACIDC, for the resolution of any potential legal, national security, publicity and privacy act issues. If the presenter has a prepared presentation, a copy will be provided along with the notification. Public Affairs Office must receive notification no later than 3 working days prior to the scheduled presentation. This requirement does not apply to routine installation fraud awareness briefings, drug awareness briefings, rape prevention briefings and other such activities.

d. As soon as possible after identifying the need to use investigative or forensic records for professionally interactive presentations, USACIDC personnel will submit a written request to USACRC, ATTN: CICR-ZA, identifying the record, its location and detailing the purpose for which the record is requested. When possible, on-site research is suggested. If records are not locally available, the USACRC will provide records necessary for research and/or the presentation. The resulting product, i.e., research paper and presentation, will be forwarded through the Public Affairs Office, to the Current Operations Branch, DCSOPS and SJA Office. The copy of the record provided for this purpose will be

destroyed upon completion of the project. Privacy act data will not be included in any research paper or presentation. All other provisions of this paragraph apply.

5-59
Procedures for release of information

a. Local CID supervisors are authorized to release information to supported PAOs based on the necessity for an immediate or time sensitive response, as appropriate, to queries from news media organizations. Supervisors will, through the respective USACIDC major subordinate command, notify the Office of the Chief of Public Affairs, HQUSACIDC, by the most expeditious means (i.e., telephone, E-MAIL, facsimile, etc.), of all information provided to PAOs for anticipated release to news media organizations.

b. In those instances not requiring an expeditious response, field element supervisors should coordinate the release of information, through the respective USACIDC major subordinate command, with the Office of the Chief of Public Affairs, HQUSACIDC.

c. Field element supervisors will release only factual and corroborated information and will not offer opinions or suppositions pertaining to any aspect of the investigation. The scope of information released should be limited to the field element's area of responsibility or supported installation. The following types of information will not be released to the PAO pursuant to inquiries from news media agencies:

(1) Classified information.

(2) Information which would compromise the investigative effort or disclose detailed USACIDC investigative techniques or procedures. However, established law enforcement procedures such as processing a crime scene for fingerprints, use of composite identification methods to describe a suspect, and types of information which could be released, provided the release does not further compromise the investigation (e.g., causing a suspect to flee the area and/or evidence to be destroyed, adversely impacting future interviews and interrogations, etc.). Release of such information must be made on a case-by-case basis taking into consideration all known aspects of the investigation.

(3) Information which would directly or indirectly identify a registered source or indicate a CID source was used in any aspect of the investigation. The term "source" will not be mentioned at anytime in the release of information to the PAO. (For example, rather than stating "The identification of the subject of this investigation was as a result of information provided by a CID source," it is recommended the release state "The identification of the subject of this investigation was made as a result of extensive and exhaustive investigation by

this office.," "...through a variety of means utilizing all available resources.", or any similar terminology.

(4) Information which would deprive an individual of a fair trial or which would be an unwarranted invasion of an individual's privacy.

(5) Information which identifies a juvenile as a subject, victim, or witness of an investigation. The status of a juvenile is determined with reference to the age of the person as of the date of the offense in accordance with applicable federal or state laws.

(6) The results of a polygraph examination and/or refusal to submit to a polygraph examination.

d. Field element supervisors should coordinate, as a minimum, with the supported SJA and provost marshal prior to the release of information to the PAO. In addition, it is recommended USACIDC supervisors advise the PAO that additional coordination by the public affairs office may be required with other installation staff elements/activities to ensure release of information serves the best interests of all parties involved.

e. The release of information pertaining to investigations being conducted jointly with another law enforcement agency (i.e., local, state, federal, host country) will be coordinated with that agency prior to release to the PAO, regardless of which agency is the lead agency. Conflicts concerning the release of information which cannot be resolved at the local level will be forwarded, through the intermediate headquarters, to the Office of the Chief of Public Affairs, HQUSACIDC.

f. All USACIDC field elements will not release any information pertaining to collateral or referred investigations and will not identify those agencies responsible for the investigations. Field element supervisors should caution PAOs that identifying other federal agencies (i.e., FBI, DEA, etc.) will jeopardize their option to utilize the glomar response. (The glomar response is a response which neither confirms nor denies the existence of information being requested.)

g. Special agents directly queried by news media representatives in extemporaneous situations such as at crime scenes will not release any information and will refer all media representatives to PAO personnel. An appropriate response to news media organizations in such situations is "I have no information to give you at this time. Please contact the public affairs officer for assistance." The terse reply, "no comment," should be avoided.

h. All media requests for formal interviews of special agents and press conferences with CID personnel when the subject matter is related to the CID mission will be forwarded, by the most expeditious means, through the appropriate USACIDC major subordinate command, to the Office of the Chief of

Public Affairs, HQUSACIDC, for approval. Approval is needed in all cases involving the CID mission, such as investigations, deployments, protective service missions, LOGSEC, criminal intelligence, crime prevention, etc. Such approval is not required if the subject matter does not relate to the CID mission, such as "man on the street" interviews or requests for a female agent's views on women's opportunities in the Army.

i. The release of information UP of this paragraph is independent of requests pursuant to the Privacy Act (PA) or the Freedom of Information Act (FOIA). Requests for information originating from news media organizations invoking the PA or FOIA will be referred, without comment, to the Chief of Public Affairs, HQUSACIDC.

j. All requests originating from news media organizations for information on investigations which have been finalized will be referred, without comment, to the Director, U.S. Army Crime Records Center.

k. All USACIDC supervisors must strive to develop and maintain an effective working relationship with their supported PAO. Concerns or conflicts concerning the release of information which cannot be resolved at the local level will be forwarded through the intermediate headquarters to the Office of the Chief of Public Affairs, HQUSACIDC, ATTN: CIIO-ZA.

5-60
General

Chapter 11, CID Regulation 385-1, USACIDC Safety Program, gives instructions to commanders and special agents-in-charge about using the risk assessment matrix (see sample at Figure E-1). Appendix E of the same reference describes the 5-step risk management process to be used during CID operations. The 5-step process is as follows:

a. Identify hazards.

b. Assess the hazards.

c. Make the operational decision.

d. Implement controls on risks.

e. Supervise and evaluate.

5-61
Objectives

a. Risk management is the application of systemic thinking to the problem of making operations safer.

b. Documenting the use of the risk management process and level of approval during CID operations is required.

5-62
Approval levels

The approval level requires a common-sense approach because of the complexity in determining the level of risk. Therefore, when in doubt about what approval level is required, brief the situation to the next higher authority for guidance. The three approval levels are:

a. High level of risk. When determined by the risk matrix and/or operations where a specific/direct threat to an individual, group of individuals and/or organization is developed will require approval by the district/battalion operations officer/commander and/or higher USACIDC level authority, as appropriate, before the operations can commence.

b. Medium (caution) level of risk. When determined by the risk matrix and/or operations where there is evidence/information of an implied threat to an individual, group of individuals and/or organization and/or the possibility of a threat to a group of individuals and/or organization will require approval by the special agent-in-charge and/or higher level of USACIDC authority, as appropriate, before the operations can commence.

c. Low level of risk. When determined by the risk matrix and/or operations where there is the possibility of a threat to an individual will require approval by the team chief and/or higher level of USACIDC authority, as appropriate, before the operations can commence.

5-63
Reducing risk level

Every effort must be made to reduce the level of risk to make the operation as safe as possible. If severe weather and faulty equipment cause the risk level to

be high, then waiting for better weather and equipment replacement may be appropriate to make the operation safer. High risk operations may have to be performed with no means of reducing the level because the operation is necessary to protect soldiers and/or their family members from harm such as terrorist activity.

5-64
Case file documentation

During CID operations when one of the above approval levels is determined to be appropriate, an entry will be made in the Agent Activity Summary documenting the results of the 5-step risk management process and/or use of the risk assessment matrix. Additionally, the approval or disapproval by the appropriate level of authority must be documented. The following is an example of an AIR entry:

> At 1100, 10 Nov 97, SA Stewart, used the 5-step risk management process to evaluate the covert drug suppression operations on PVT Woodman and a high level of risk was determined. This operation was discussed with CW4 Irene Kauker, District Operations Officer, who approved the operation.

5-65
General

The guidance contained in this section prescribes policies and procedures for investigating and reporting violations of the rules of engagement by USACIDC personnel during operations other than war. When in contradiction, this policy supercedes policies detailed in chapter 7 of this regulation.

a. Definitions.

(1) Rules of engagement. Directives issued by competent military authority that delineate the circumstances and limitations under which US forces will initiate and/or continue combat engagement with other encountered forces.

(2) Senior U.S. Military Commander. The senior U.S. Military Commander responsible for all military operations in a particular theater of operation. The senior military commander may delegate resolution authority for violations of rules of engagement to a subordinate task force commander for that operation. This definition describes that commander responsible for adjudicating all violations of rules of engagement.

b. Policy.

(1) All USACIDC personnel deployed in operations other than war will adhere to the rules of engagement established by the senior U.S. Commander for that theater of operation.

(2) The first general court-martial convening authority in the chain of command is the final authority and action commander for all decisions regarding punishment under the UCMJ for violations of the rules of engagement by USACIDC personnel.

c. Procedures.

(1) All alleged or reported violations of rules of engagement by USACIDC personnel will be investigated in accordance with the following CID policy in addition to procedures established by the senior military commander for that operation.

(2) A preliminary investigation will be initiated into all alleged or reported violations of the rules of engagement, including the use of deadly force, by USACIDC personnel. The preliminary investigation will result in one of the following findings, after coordination with the supported staff judge advocate for that operation:

(a) A determination that a violation of the rules of engagement did not occur. In this case, the sequence number action will be completed and the investigative effort documented in the AAS.

(b) A determination that a violation of the rules of engagement did occur. In this case, the senior USACIDC commander on location must decide if the violation was justified under the circumstances. In making this determination the USACIDC Commander should consult with the staff judge advocate supporting the operation. If the USACIDC Commander determines the violation was justified, no further action is required. The preliminary investigation will be terminated with the results documented in the AS. If the USACIDC commander determines the violation was not justified, a ROI will be initiated for violation of a lawful general order or regulation (Article 92, UCMJ), and any other offense(s) which may also have been committed. Upon initiation of a ROI wherein a violation of Article 92 is the only offense involved, the decision on whether to suspend performance of investigative duties, to include withdrawal of the badge, credential, and weapon is the responsibility of the senior USACIDC commander on location, taking into consideration the totality of the situation and all attendant circumstances. If, in addition to a violation of a lawful general order or regulation, credible information exists that a criminal offense (e.g., murder, manslaughter, etc.) was also committed, the USACIDC commander on location will:

1. Suspend the individual from all investigative duties.

2. Temporarily withdraw the individuals badge, credential, and assigned/issued weapons(s).

3. Ensure immediate return of the individual to a rear support area in the theater of operation or redeployment of the individual, as deemed appropriate. Redeployment of the individual from the theater of operation under these circumstances should only be considered if the ROI results in a founded criminal offense(s).

d. Reports.

(1) Reported incidents or suspected violations of rules of engagement by USACIDC personnel may be reported by SSI only if deemed appropriate by a USACIDC supervisor based on the nature of the incident and totality of the circumstances. Subsequent SSI status reports may be submitted, as appropriate, upon receipt of additional information.

(2) All violations of the rules of engagement by USACIDC personnel which result in the initiation of a ROI will be reported by initial/SSI as expeditiously as possible. Subsequent status/SSI reports will be submitted, as appropriate, upon receipt of additional information.

(3) Copies of final ROIs will be distributed as follows:

(a) Senior U.S. Military Commander or delegated representative for the respective operation (action commander).

(b) Supported staff judge advocate for the respective operation

(c) HQUSACIDC

(d) USACRC

(e) Appropriate USACIDC major subordinate command headquarters.

(f) File

d. Applicability. This policy guidance applies only to incidents in which USACIDC personnel are directly involved in alleged or reported violations of the rules of engagement. This guidance is not in contravention with the policy guidance outlined in paragraph 5-22, regarding the reporting of casualties during operations other than war.

5-66
General

The guidance in this section prescribes the policies and procedures for reporting cooperation with civilian law enforcement officials as required by DoD Directive 5525.5. DoD Directive 5525.5 requires the Department of the Army to cooperate with civilian law enforcement agencies to the greatest extent possible without violating the limitations of the Posse Comitatus Act. Appendix F describes the type of assistance which is authorized, the appropriate approval level for requested assistance, the reporting requirement through CID channels, and the reporting format.

CHAPTER 6

6-1
Documentation

a. The documentation of investigative effort is required to provide information to supported commanders, CID supervisors, and other authorized recipients of law enforcement information. Because this information forms the basis for many decisions which affect lives, privacy, and property, the documentation of CID investigative information and activities must be accurate, thorough, and timely.

b. Documents must be provided promptly to those who are authorized to receive them, and must be scrupulously denied to those who are not. See chapter 8 for information on distribution and chapter 25 concerning the release of information.

6-2
Sequence numbers

a. Sequence numbers are control numbers enabling the identification and tracking of activities and workload data directly related to specific criminal investigations, complaints, crime prevention surveys, protective service missions, and programs in direct support of investigative operations. They are not intended to be applied to administrative actions, housekeeping functions, duty officer details, unit training, liaison activities, routine suspense control numbers, or other activities not described in this paragraph.

b. The sequence number consists of three groups of digital information separated by hyphens. The first group is a four digit sequential number assigned by the originating USACIDC element and the sequence begins at 0001 on the first day of each year; the second group is the year of initiation of the action, and the third group is the USACIDC unit number. The sequence number appears as follows:

0115-93-CID065

c. Sequence numbers will be assigned when an action is initiated. The sequence number action is initiated when:

(1) A USACIDC unit receives an indication, by whatever means or from whatever source, of an alleged criminal incident which is, or may be, within USACIDC's investigative responsibility. If any investigative activity is required to determine whether or not the incident is within USACIDC's investigative responsibility, a sequence number action will be opened.

(2) A crime prevention survey is initiated.

(3) A criminal intelligence report is prepared.

(4) Investigative responsibility is assumed from a subordinate USACIDC element or as a result of a control transfer investigation.

(5) A request for assistance (RFA) is received from another USACIDC or other law enforcement element except where the request can be verbally answered with minimal investigative effort (see paragraph 7-24). When an RFA is received which pertains to an ROI on which a previous RFA was worked and that file closed, a new sequence number will be assigned to this RFA except when the response can be verbally answered with minimal investigative effort. An RFA limited to the correction of administrative deficiencies in previously prepared Information Reports such as unsigned statements, missing/incomplete CID forms, etc., should not be documented under a new sequence number. This request should be processed as a non-investigative administrative action.

(6) A tasking is received for a protective service mission.

(7) A complaint of a criminal offense outside USACIDC's investigative authority is received and relayed to another investigative authority, requiring significant effort by the receiving office. Otherwise, the complaint can be documented in a raw data folder.

(8) A criminal intelligence raw data folder (i.e., general, economic, drug or combinations as appropriate) is prepared. The duration for the file to be maintained as an open action is at the discretion of the special agent-in-charge. One folder can be opened monthly, quarterly, semiannually or annually, and tabbed to index general, economic and drug criminal intelligence (raw data); fraud awareness briefings; and drug awareness briefings as appropriate to meet the needs of the investigative unit. The file duration to receive information and category(s) of raw data to be placed in the file should be based on amount of information received and the ability to organize the file folder in a retrievable manner. The investigative unit can elect to open individual folders for briefings if large numbers of briefings are given.

(9) A Target Analysis File and/or other type of economic crime target analysis action.

(10) A formal crime analysis of general crime(s) is prepared.

(11) Training relating to investigative programs is provided to supported units.

(12) Requests for polygraph examinations are received from military police or defense counsels.

(13) As directed by investigative supervisors in situations meeting the general criteria of this paragraph.

d. Once assigned, a sequence number will not be reassigned.

6-3
Report of Investigation (ROI) numbers

a. ROI numbers are utilized by the USACRC for filing, indexing, information storage, and data retrieval. ROI numbers must be annotated on all documents forwarded to USACRC.

b. ROI numbers are assigned when a formal criminal investigation is initiated in the ACIRS.

c. The ROI number consists of five numerical digits and is appended to a sequence number assigned in accordance with paragraph 6-2. Sequence and ROI numbers are separated by a hyphen and appear as follows:
0001-01-CID001-00001

d. An ROI number will not be reused once it has been assigned, unless authorized by the USACRC due an error (i.e., ACIRS transmission of a sequence action as an ROI).

6-4
Offense code

An offense code or codes will be assigned to each initial, initial/SSI, status, final, collateral, referred, supplemental, crime survey, and criminal intelligence report at the time the report is prepared. Each offense, to include unfounded offenses, listed in the subject/victim section of the report will be included in the offense code. If more than one code applies to a specific offense, all applicable codes will be shown to include supplemental codes such as laboratory examinations. The primary offense code is the most serious offense being investigated, and that code will be the first code used in the sequence of offense codes on the report. A listing of offense codes and primary offense code instructions are provided in appendix A and chapter 7 of this regulation. The offense code(s) will be appended to the sequence number or sequence with ROI number and appears as follows:

Sequence number only action:
0001-01-CID001-9H

ROI action:
0001-01-CID001-00001-7C2H/7F5A1

6-5
Requirement

A CID Action Record (CID Form 66) will be initiated whenever a sequence number action is opened.

6-6
Preparation

The CID Form 66 is generated from the ACIRS after a file has been opened.

6-7
Use

The CID Form 66 is designed for internal use and should not be released outside USACIDC unless there is an overriding reason. When there is a need to forward the results of a preliminary investigation which has been completed as a sequence number only action, the procedure described in paragraph 4-8 will apply.

6-8
Completion

The CID Form 66 is completed when the ACIRS file is closed.

6-9
Requirement

A case folder will be prepared for each sequence number action.

6-10
Filing

Filing and disposition instructions for the case folder are in AR 25-400-2. All CID elements will disregard the guidance for file number 195-2e stated in AR 25-400-2, The Modern Army Recordkeeping System (MARKS). File number 195-2e will be assigned to all reports concerning statistical and analytical data, crime prevention surveys, threat assessments and vulnerability assessments. The following revised instructions will be used:

File Number: 195-2e

Title: CID investigative activities reports

Description: Statistical and analytical reports concerning CID activities, crime prevention surveys, threat assessments, vulnerability assessments and other survey or assessment type reports.

Disposition: Destroy in current files area (CFA) after 3 years unless needed for further reference or intelligence purposes.

6-11
Preparation

The preparation of the case folder is controlled as follows:

a. The CID case folder will consist of a folder containing the CID Action Record, an Agent Activity Summary, other related forms, and documents (ROI, Agent Investigation Report, Evidence Vouchers, statements, photos, etc.) accumulated during the investigative activity.

b. The sequence number will be properly displayed on the CID case folder for identification and filing. The sequence/ROI number will be properly annotated on all documents within the case folder.

c. The CID Form 66, with attached MPR, incoming request for assistance, or other document which caused the CID Form 66 to be prepared, will be filed as the uppermost document on the right side of the folder. The final ROI will be filed under the CID Form 66. Initial and status reports are filed under the final report in chronological order, from bottom to top. The Agent Activity Summary (AAS), Agent Investigation Report (AIR), interview work sheets, and all other documents, notes, photographs or negatives (when not attached as exhibits to an ROI or a declination MPR) will be filed on the left side of the folder. (See figures 6-1 and 6-2).

d. Draft documents will be maintained in the case folder and replaced when the final is typed. When documents are dictated, this requirement is not applicable.

e. Notes prepared by special agents will be maintained in the case folder until final disposition of the folder.

f. Multi-folder files

(1) For those ROIs, Information Reports, etc., with a large number of documents, more than one working folder may be used with each folder being numbered, i.e., folder 2 of 9 AAS, folder 3 of 9 narrative, folder 4 of 9 AIRs, folder

5 of 9 RFA, folder 8 of 9 Evidence Vouchers, etc. The first folder should contain the CID Form 66 and final ROI/information report(s) when possible.

(2) When the final ROI, information report, etc., has been completed, the folders should be reorganized so that the final ROI/Information report/document is in the first available folder(s) (with or following those that contain the CID Form 66 and AAS).

(3) These multi-folder files should include an index on a CID Form 28 or bond paper (i.e., folder 2: ROI thru Exhibit 55, folder 5: interview work sheets, etc.) as the top document on the left side of folder 1 except when a suspended document pertaining to action taken is pending a reply, in which case this document may be the top document until final action is completed.

6-12
Release of case folder

The case folder is for internal CID use only and is not normally released outside of CID channels. Persons may be authorized to review the case folder and its contents; copies of related documents or reports contained therein may be released to authorized individuals; however, the case folder will always be maintained in the personal custody of a CID special agent or within the files system of the CID office. The case folder **will not** be released without specific authorization of HQUSACIDC, in response to a court order, or to a ruling by a military judge. Release of information will be in accordance with chapter 21 of this regulation.

6-13
Case File Storage

a. All USACIDC elements are granted an exception to AR 25-400-2, The Modern Army Record Keeping System (MARKS) policy wherein, at the discretion of the group commander, investigative files may be retained at the Resident Agency level for the entire retention period prior to destruction, rather than being transferred to the district or field office.

b. In implementation of exception, Resident Agencies assuming responsibility for storage also incur responsibility for destruction at the end of the retention period.

6-14
Purpose

The ACIRS is the basic control to account for CID operational actions. In the absence of ACIRS, the Consolidated Complaint/Case Log (CID Form 54) can be used as an alternate method.

6-15
Requirement

All USACIDC units, except USACIL, will maintain:

a. ACIRS; or,

b. CID Form 54; or,

c. If the ACIRS is not yet installed or operational, an automated computer program approved by HQUSACIDC, that captures the same data information required in the CID Form 54. If an automated system is used, a back up disk will be prepared daily and maintained to ensure that only a minimum of data would be lost in the event of system/program failure. A monthly hard copy printout will also be maintained as a back up file.

6-16
Preparation

The preparation of the manual CID Form 54 will be in conformity with the following:

a. An entry will be made on CID Form 54 for each sequence number assigned.

b. A line may be skipped between entries, if desired. More than one line may be used for a voluminous entry.

c. A new volume will not be initiated at the beginning of each calendar year. All useable pages in the volume will be filled. The dates covered in the volume will be identified on the cover.

d. Entries will be made in ink unless otherwise directed. Erasures, line outs, or correction fluid may be used to correct errors.

e. The following data is required when appropriate; additional data may be entered; color coding is authorized, but not required:

(1) CID sequence number and date received. Sequence numbers will be entered in numerical order. The "Date" is the date the USACIDC initiated the action. Normally these dates will be in chronological order.

(2) MPR number. Enter the MPR number when known and include the year the MPR number was assigned, if not the same as the current calendar year.

(3) ROI number and date assigned. Enter the five digit case number, if any, and the date assigned.

(4) Date of incident. Enter the date the incident occurred. This may, when appropriate, be reflected as "Unknown" or as a time span (e.g., "May-Nov 85").

(5) Offenses. Enter the primary offense. Additional offenses may be entered if desired. When an action is not related to a criminal offense, enter a word or phrase descriptive of the action.

(6) Subjects. The following entries are appropriate for the subject column:

(a) For preliminary inquiries/investigations, enter the last name of the primary subject. Additional names or identifying data may be entered. For multiple subjects, enter the name of the primary subject and the phrase "and several others", et al, or the names of all subjects. The words "Unknown" and "None" may be used when appropriate.

(b) For protective service missions, the last name of the principal (protected person) or position title will be entered.

(c) For crime prevention surveys, the subject matter of the survey or the facility being surveyed will be briefly identified (e.g., "Increase in armed robbery at post gym" or "Ft. Campbell Officers Open Mess").

(d) For criminal intelligence reports, the name of the individual involved or the subject matter will be entered.

(e) Companies or firms will be listed by the company or firm name.

(7) Victim. If applicable, enter the last name of the primary victim. Additional names or identifying data may be entered. The words "Unknown" or "and others" may be used.

(8) Agent. Enter in pencil the last name of the special agent or designation of the team (e.g., persons, drugs, general crimes, A, B, etc.) to whom responsibility for the action is currently assigned.

(9) Status. Record the type and date of reports. Only the initial, final and supplemental reports must be recorded and will be in ink. Entries relating to status ROI may be made; if so, they will be in pencil and erased when the next entry is made.

(10) Remarks. The remarks block is to be used as determined locally. It may be used to cross-reference, to explain erroneous entries, or to serve as a memory "trigger" to aid in the recollection of the specific incident.

6-17
General

The procedures explained in this regulation provide for the accounting and documenting of all CID actions. It is recognized that CID supervisors will utilize various management techniques, depending on unit size, organization, area of responsibility, and personal management experience, to ensure thorough and timely investigative effort, and timely and accurate processing of CID reports.

6-18
Case status board

A case status board may be used to control and account for CID actions. The size and construction of the board should be determined locally consistent with the number of special agents assigned, investigations opened, and other organizational requirements. A case status board is not a requirement and other options such as an automated criminal investigative case management system may be used to more effectively or efficiently manage cases and workload data

6-19
Investigative plans

a. Investigative plans are essential to the successful management of any significant criminal investigation. Once prepared, they must be reviewed frequently, evaluated, and modified or revised as necessary to meet the requirements of evolving investigations. It is not necessary and not required that such a plan be prepared for every investigation undertaken by USACIDC units. They should, however, be prepared for any major or complex investigation (e.g., homicides, major fraud investigations) or when deemed desirable by a CID supervisor (e.g., as a practical instructional aid for special agents.)

b. The exact contents of an investigative plan will vary according to the circumstances of a particular investigation, thus a single prescribed format will not suit the needs of all situations. Emphasis must be on flexibility and

adaptability. As each individual element of the plan is accomplished, the date of completion should be entered beside that element. The following is a suggested format which should be modified as necessary to meet existing requirements. (Elements which are not needed may be deleted; others, not listed, may be added to meet particular circumstances.

(1) Alleged offenses under investigation with elements of proof of each.

(2) Evidence which will establish each element of proof.

(3) Persons to be interviewed (victim, witness, subject) and when in the overall investigation each should be interviewed.

(4) Investigative analysis. What is the impact on the Army (i.e., safety, readiness, monetary, etc.), chronology of events, corporate/individual asset determination (civil action), and/or anticipated defenses.

(5) Other law enforcement agencies with which coordination may be necessary.

(6) Legal coordination required (SJA, U.S. attorney, DPFU, procurement fraud advisor, etc.) and when this should be accomplished.

(7) Special investigative assistance which may be required (auditors, technical listening operations, crime laboratory, polygraph, other forensics, technical experts) and when each will be required.

(8) Special logistics and administrative support required and when it will be needed.

(9) Date of preparation of the investigative plan or date of most recent revision.

c. When used, investigative plans should be prepared on plain bond paper or AAS and filed as the top most document on the left side of the case file to allow for easy reference and review.

6-20
Case review

a. CID unit review. Review of the finished report must begin with the assigned case agent at the time of preparation of the report. The agent must ensure that the report portrays the total investigative picture clearly and accurately, and in a manner which will reflect creditably upon the preparing agent and the originating unit. It must show, to individuals miles away and perhaps years later, the facts or circumstances of the particular investigation. The report must be able to

withstand the scrutiny of those who would wish to deny or defend against the facts contained in it. The finished report is the "end product" of the USACIDC. The report must reflect the highest standards of quality and professionalism. The final product must be closely reviewed for content, accuracy, and typing errors.

b. Supervisory review

(1) Supervisory review of CID reports will be conducted at level(s) above the preparing office, and the Crime Records Center. Some reports will be reviewed at all levels and in great detail, while others will be less closely scrutinized or only spot checked. In whatever case, the review procedure must be timely to ensure the rights of the individual and the U.S. Government are protected.

(2) Supervisory review may result in the return of reports for correction or modification. When this is necessary, the preparing unit is faced with the problem of correcting other copies of the report already in distribution locally. Review and correction procedures must be accomplished and the corrected report returned without undue delay.

(3) Supervisory review of CID reports is facilitated by the reviewers having a detailed, technical knowledge of the mechanics of CID report writing. However, the review must first assure that the report serves its primary function: the reporting of the facts for command action. Once this is done, attention should then be directed to the mechanics of the report itself.

6-21
Quality control procedures

A thorough and timely review of all completed reports is required. This review may be conducted at any level which ensures objectivity. This review will normally be done subsequent to the dispatch of the report by the preparing office and should not delay the investigative process.

a. Each USACIDC major subordinate commander will ensure that a quality control review is done for each completed ROI. The level where this review is done will be at the USACIDC major subordinate commander's discretion so long as the review ensures objectivity. It is not the intent or purpose of this regulation to establish or require a 100% review at the USACIDC major subordinate command level.

b. Review of ROIs completed at the investigative level will require a second level review of a copy of the report at a higher headquarters unless a specific written exception is granted by the USACIDC major subordinate commander. The original ROI will be forwarded directly to the USACRC and not through a higher level office so not to delay the original report to the USACRC.

c. HQUSACIDC will select and review SSI reportable, monitorship, and DIMIS ROIs and conducts 100% review of certain categories of cases. This review is not in lieu of a field review. If deficiencies are identified, the report will be returned to the appropriate major subordinate command for necessary corrections.

d. An administrative review of all ROIs will be conducted at the Crime Records Center upon receipt and processing of all original final reports.

e. HQUSACIDC will periodically identify certain reports for review to monitor the effectiveness of the field review of CID reports. Reports for this review may be identified by specific crime category or by limited geographical areas and will be identified to the field elements.

6-22
Law Enforcement Availability Pay (LEAP)

a. Purpose: This paragraph revamps USACIDC policy on LEAP based on recommendations by the HQUSACIDC, Internal Review report, subject: Review of Law Enforcement Availability Pay Documentation Procedures within the Major Procurement Fraud Unit, 701st Military Police Group (CID), Fort Belvoir, Virginia, 6 Aug 98. The Office of Personnel Management (OPM) regulations implement the statute and are published in 5 C.F.R. §§550.181 – 550.187.

b. Policy:

(1) Initial eligibility for LEAP. Eligibility for LEAP will begin for all newly hired criminal investigators upon graduation from the Apprentice Special Agent Course, U.S. Army Military Police School. Criminal investigators transferring to the USACIDC from other Federal law enforcement agencies will be eligible for LEAP upon verification by USACIDC, Deputy Chief of Staff for Support (DCSSPT) that they were an accredited criminal investigator with a former Federal agency.

(2) Annual agent certification. The OPM requires an annual certification from agents and their supervisors that the agents currently meet and are expected to meet the substantial hours requirements of LEAP (§550.184). These statements will be forwarded by the supervisors of LEAP recipients to the major subordinate commands (MSCs), where they will be retained.

(3) Quarterly review. It is the obligation of the USACIDC, through its supervisors, to ensure that agents can meet their substantial hours requirement (§550.182(d)). To accomplish this, supervisors will review agent status quarterly. Section 550.183, provided in the appendix, describes the required computation

process. The supervisor will record the results of the calculations described in §550.183(b)(3). The results of the quarterly calculations will be forwarded to the MSCs where they will be reviewed and maintained.

(4) Failure to meet substantial hours requirement. If an agent is not on track to meet the substantial hours requirement, the supervisor and the agent will establish a course of action to ensure that the agent will meet the annual requirement. This course of action should be a written plan of assistance by the supervisor, developed after quarterly reviews to allow adequate time and supervisory management to track the annual average of 2 hours of unscheduled duty per day.

(5) Suspended duties. If an investigator entitled to LEAP is suspended from duties, the responsible supervisor must determine whether the suspended investigator's unscheduled duty hours are or will be sufficient to enable the investigator to meet the substantial hours requirement and make required certification. A finding that an investigator will be unable to perform unscheduled duty (availability or work) as assigned, will be grounds to deny or cancel certification. The denial or cancellation of LEAP is an adverse personnel action. The MSC commander is the approval authority to deny or cancel certification based on supervisory recommendation that is approved by legal and civilian personnel office review. Additionally, suspension of LEAP must document the length of the suspension, work and pay requirements, handling of deficit hours and recertification procedures/conditions to suitably advise the investigator.

(6) Review prior to training. Agents will not be disadvantaged because of attendance at USACIDC approved training (§550.183(b)(3)). Supervisors will ensure that the agent has completed sufficient unscheduled duty hours to ensure that the agent does not begin training with a deficit in hours. Agents attending USACIDC approved training will receive LEAP during the training. As part of the calculations required by §550.183(b)(3), training days are considered excludable days.

(7) Rounding time expended on tasks performed. Investigators will round time expended on tasks up or down to the nearest quarter hour.

b. Supplementation of this policy. The MSCs will establish dates when the quarterly reviews will be received, what supporting documents will be required and which staff section will be responsible for reviewing the submissions. Any further supplementation of this policy must be coordinated with the office of the staff judge advocate, HQUSACIDC and approved by the

6-23
Sex Crimes/Child Abuse Monitorship

a. General. This paragraph establishes policy for the implementation of a monitorship program of sex crimes and child abuse investigations at the district, group, and headquarters levels. Given the unique nature of these types of cases, monitoring will ensure compliance with established policy and recognized investigative techniques.

b. Responsibility. A senior agent will be assigned monitoring responsibility for all sex crime/child abuse investigations initiated by subordinate investigative units. This position will be initiated at the battalion, group, and HQUSACIDC levels. At HQUSACIDC, monitoring will be performed by the Chief, Persons Branch, Current Operations, ATTN: CIOP-COP-PE.

c. Policy

(1) Agent assigned such responsibilities should be a senior member of the command and should have attended subject specific training such as:

(a) Child Abuse Prevention Investigative Techniques (CAPIT) Course

(b) DA Family Advocacy Staff Training Course - Advance

(c) DoD Family Advocacy Staff Training Course

(d) DoD Family Advocacy Command Assistance Team (FACAT) Course

(2) Monitorship should assure uniformity in policy and technical procedure regarding the conduct of sexual crime and child abuse investigations throughout the command.

(3) Selected on-going and completed investigations should be reviewed for quality control purposes and to identify both positive and negative results of techniques employed in conducting these investigations.

(4) Systemic problems or training/resource deficiencies should be brought to the attention of HQUSACIDC for discussion and resolution.

CHAPTER 7

7-1
Purpose

The CID report of investigation (ROI) is the basic means of providing the results of investigative activity to supported commanders for information purposes and administrative/disciplinary action, to CID supervisors for information and quality control, and to the U.S. Army Crimes Record Center (USACRC) for criminal information and long-term maintenance of investigative data. The ROI reflects information on persons, corporations, or other legal entities, which have committed or are suspected of committing crimes under the investigative jurisdiction of the USACIDC as outlined in AR 195-2.

7-2
Classification of USACIDC reports

All USACIDC reports are exempt from disclosure under the Freedom of Information Act of 1974 and will be marked "For Official Use Only," as a minimum. Termination of protective markings is exempt in accordance with chapter 3, AR 25-55.

a. USACIDC reports will be classified if they contain material or information already classified by another agency. When this occurs, the CID report will be classified in IAW AR 380-5. In such cases, the classifying agency or source will be consulted to ensure that the proper classification markings and downgrading instructions are placed on all CID documents.

b. USACIDC reports may be considered for a higher level of classification because of the nature or sensitivity of the information contained therein. Procedures for classification authority are established in AR 380-5 and are applicable to USACIDC reports. All USACIDC major subordinate commanders (MSC) have authority to classify report as "CONFIDENTIAL" and the Commanding General (CG), USACIDC, has the authority to classify to "SECRET". Authority for setting a higher classification will be IAW AR 380-5.

c. Whenever a CID report is classified, the same level of classification is applicable to the entire CID case file and associated documents.

d. Classified information will not be entered into the Automated Criminal Information Reporting System (ACIRS); however, available unclassified data will be entered into the ACIRS to generate a sequence number and/or ROI number if applicable. In this regard, attention must be given to the fact that while individual data elements may be unclassified, they may become classified when combined in a single file or document. An example is that a unit designation and a geographic location may both be unclassified, but may become classified when

combined as a unit address. The data elements required by the ACIRS to open a sequence numbered action are the "Type of Action" and the "serious or sensitive information" (SSI) flag. Neither of these data elements should ever be classified. An initial ROI must be created within the ACIRS to generate a ROI number. The required data elements to create an initial ROI are the "Incident Date," "Subject Name," and "Investigative Summary." If the "Incident Date" is classified, the date the action was initiated should be used. Edits within the ACIRS require the "Incident Date" to be a valid date between 1 January 1801 and the date the action was initiated. If applicable, the word "CLASSIFIED" may be entered into the "Subject Name" field. No other biographical data need be entered if the identity of the subject is classified. Likewise, the "Investigative Summary" may be limited to a one-line entry such as, "This investigation is classified." All reports containing classified information must be prepared outside of the ACIRS.

e. All classified reports will be handled, stored, and transmitted IAW AR 380-5.

f. Offices having CID case files that are classified must have an indexed retrieval system to search for data contained in classified investigations. The retrieval system must be handled and stored IAW AR 380-5.

7-3
Preparation

Investigative reports are USACIDC's primary "products" and constitute the only enduring record of activities that have far reaching impact. Poorly written reports can largely nullify the productive results of hard work, perseverance, and initiative. It is important, therefore, that those that prepare and review CID reports strive to improve the quality of written reports. There are many publications on writing improvement, including DA pamphlets, which may be consulted for guidance. Investigative reports in particular; however, should be written in accordance with several basic principles:

a. Pertinent. Only information pertaining to the offense or the investigative effort undertaken should be recorded in the ROI. Housekeeping activities and activities which are purely administrative (e.g., "SA X drove to the orderly room in an effort to locate Y." should normally not be recorded in the ROI. Only in exceptional circumstances, which could have an impact on the credibility of the investigation (e.g., significant delay in locating a critical eyewitness), should such matters be addressed in the ROI. In addition, redundancy should be avoided. In a larceny case, for example, a full description of the items stolen, to include stock numbers and serial numbers, should be documented in the appropriate Agent's Investigative Report (AIR) and not the ROI's investigative summary. Needless repetition of details merely hinders comprehension. Judgment must be exercised to recognize what should be reported and where the information should be documented. Make, model, color, identification number, etc., seldom

demonstrate elements of proof and need not be documented in the investigative summary of the ROI. Values of property or damage; however, are required to demonstrate the commission of certain crimes and must be documented in the investigative summary.

b. Accurate. Although it is a basic assumption that reports are accurate, it should be realized that even comparatively minor discrepancies may give the impression of inaccuracy. Inconsistent details such as times, descriptions, numbers, differing accounts by the same witness when interviewed by different agents which are not resolved, etc., give the appearance of carelessness and cast doubt on the credibility of the entire report.

c. Clear. Not only should each sentence be understandable, but the ROI as a whole should tell a coherent story with smooth, logical transitions. It must also be remembered that ROIs are maintained for long periods of time and are often consulted years after being written. Terms that are common at one time and place may be incomprehensible 10 years later or in a different locale. Although some documents, particularly sworn statements, should reflect the actual language used by its author, clear explanations must be provided for acronyms, abbreviations, slang, unit designations, foreign terms, etc. Lack of clarity has a significant impact on decisions made by the staff judge advocate (SJA) and supported commanders. When appropriate, such clarifications can be made by asking further questions within the body of the statement made or as an “Agent’s Comment:"

d. Unbiased. Not only must the investigation be conducted in a fair and impartial manner, this impartiality must be reflected in the ROI. Failure to follow up leads or resolve issues raised during the course of the investigation may give the impression of individual biases which might not be indicative of a professionally conducted criminal investigation.

e. Comprehensive. A ROI must answer all essential questions about an incident. All elements of proof must be clearly documented. The reader should not be required to make assumptions resulting from lack of information. It is essential that the ROI be complete and capable of standing alone. It must provide the ultimate user(s) with all information needed to initiate and complete any disciplinary or administrative action without referring to the case agent or CID case file for clarification or additional information.

f. Approval. In order to ensure accuracy in reporting and compliance with the provisions of this regulation, all CID reports of investigation (i.e., initial, status, final and supplemental) will be reviewed and approved by the Special Agent in Charge or the designated next-in-line supervisor. Further delegation of this authority is not authorized.

7-4
Subjects

a. A subject is a person, corporation, or other legal entity (hereafter referred to as "person"), about whom credible information exists to believe committed a particular criminal offense. The acts of titling and indexing are administrative procedures and do not connote any degree of guilt or innocence. A person listed as a subject may be deleted from the ROI only under the following circumstances:

(1) In the case of mistaken identity, i.e., the wrong person's name was placed in the report of investigation as a subject or entered in the DCII.

(2) When an error was made in applying the credible information standard at the time the initial or status ROI titling the person was initiated, but not after subsequent investigation determines that credible information does not exist. If an error in applying the credible information standard is later identified during operational review or the amendment process, the original listing of the person may be viewed as an administrative error and corrected through deletion.

(3) The credible information standard is applied only to decisions to list a person as a subject of a ROI. It should not be confused with the probable cause standard used to determine whether the offense reported was founded, unfounded, or insufficient evidence.

b. Army members who are under investigation by law enforcement agencies for possible criminal violations must be suspended from receipt of favorable personnel actions ("flagged") in accordance with AR 600-8-2. Although personnel policy in this regard is contradictory, precedent exists to apply the term "favorable personnel action" to discharge from the Army for any reason (ETS, resignation, retirement, etc.) without meeting the traditional criteria of referral of criminal charges. When the subject of a ROI is allowed to leave military control or transfer from the unit of assignment at the time of initiation of a ROI, the investigation and subsequent attempts to take action against the offender are often adversely affected. USACIDC reports on known subject cases, other than final and final supplemental ROIs, will include a paragraph to remind commanders of their responsibility as outlined in AR 600-8-2, pertaining to suspension of favorable personnel actions and AR 380-67, for the suspension of security clearances.

c. The determination for listing a person as a subject is based upon a credible information standard. Credible information is information disclosed or obtained by USACIDC that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to lead a trained investigator to presume that the fact or facts in question are true.

d. The decision to report a person as a subject must be made only after a careful assessment of the information and the credibility of its source. In every instance, the circumstances, known veracity, or possible motive of a complainant must be considered.

e. The decision to report a person as a subject will be made and approved by a CID supervisor. While it is necessary to coordinate investigations with the SJA or U.S. attorney, the decision to list a person as a subject is the responsibility of the USACIDC.

f. In overseas areas, civilians may be listed for extraterritorial provisions of the United States Code (USC) as well as violations of local law.

g. A service member who commits an offense, and is subsequently discharged, will be listed for the appropriate Uniform Code of Military Justice (UCMJ) offense.

h. The ROI is a “case based” report; however, USACIDC must report “incident based” data from each ROI to the Defense Incident-Based Reporting System (DIBRS). Subject data must be reported for each subject under investigation when:

(1) The entry "Unknown" will be used if the subject of a ROI is not identified.

(2) If a victim reports a crime involving more than one unknown perpetrator, “Unknown” must be listed consistent with the number of subjects reported. As an example, if a victim reports being assaulted by two unknown subjects and then raped by a third, the ROI must list "Unknown” as subjects 1, 2, and 3. This procedure allows the linking of subjects to specific offenses. Additional data pertaining to an “Unknown” subject can be recorded as it becomes known.

7-5
Victims

a. The victim of a crime against persons (e.g., murder, robbery, and aggravated arson) is the person who suffered the injury or who was put in danger or fear by the criminal act.

b. The victim of a crime against property (e.g., larceny, forgery, and housebreaking) is the owner of the property involved.

(1) The owner of private property is the person, corporation, or other legal entity commonly viewed as having ownership, regardless of security interests (e.g., liens, mortgages) held by others.

(2) The owner of U.S. Government property is the U.S. Government. Further identification by agency, activity, or unit down to company/battery/troop level will be made in parentheses (i.e., U.S. Government, (A Company, 71st Ordnance Battalion), Fort Example, FL 33141). Individuals having a personal responsibility for U.S. Government property entrusted to them for their exclusive personal use will also be listed as victim. If more than one victim unit is involved, the U.S. Government will be listed as a victim accordingly.

(a) The victims of housebreaking or burglary in U.S. Government quarters will be both the U.S. Government and the assigned occupant.

(b) The victims of larceny of an individual's field equipment will be both the U.S. Government and the individual who is responsible for the equipment.

7-6
Investigations and offenses

a. Primary offense. The overall categorization of a final ROI is determined by the results of the investigation as it relates to the primary offense. The primary offense is the most serious offense investigated, based on the maximum punishment listed in the UCMJ, USC, or an applicable state or foreign statute. Where more than one offense carries the same penalty, offenses against persons will be considered more serious than offenses against property. Where more than one offense in the same category (i.e., persons or property) carries the same maximum punishment, the offense that occurred first is the primary offense. The primary offense may change to a more serious offense during the course of an investigation to reflect new findings or events; however, the primary offense will never revert to a less serious offense. If the primary offense is determined to be unfounded, but a less serious offense has occurred, the more serious offense will remain the primary offense.

b. Categorization of investigations (solved or unsolved). The categorization of a case is based on all facts and circumstances present at the time the investigation is completed and the final ROI is prepared and is a decision made by the investigating USACIDC unit, independent of any judicial opinion or disciplinary action. All subjects of the primary offense need not be identified to categorize a case as solved.

(1) Solved. A determination made by the USACIDC upon completion of the investigation that:

(a) The primary offense of the ROI is a founded offense and investigation established probable cause to believe a person listed in the subject block of the ROI committed the primary offense, or

(b) The primary offense is determined to be unfounded.

(2) Unsolved. A determination made by the USACIDC upon completion of the investigation that:

(a) The primary offense of the ROI is a founded offense and a person has not been listed as a subject of the primary offense, or

(b) Investigation has not established probable cause to believe a person listed in the subject block of the ROI for the primary offense committed the primary offense. Although another offense may have been committed in addition to the primary offense and a person is listed in the subject block for committing the other offense, if the investigation did not establish probable cause to believe that a person committed the primary offense, the overall classification of the investigation is unsolved.

c. Categorization of offenses:

(1) Founded. A determination made by the USACIDC that a criminal offense has been committed. The determination that a founded offense exists is an investigative decision independent of any judicial opinion or disciplinary action.

(2) Unfounded. A determination made by the USACIDC that a criminal offense did not occur. This determination must be based on demonstrative evidence that the offense did not occur. A lack of evidence to support a complaint or questioning of certain elements of a complaint is not sufficient to categorize an incident as unfounded. A finding of insufficient evidence is not a basis for unfounding an offense.

(3) Insufficient evidence:

(a) The inability of the investigation to determine that a reported or alleged criminal offense did or did not occur, or

(b) The inability to establish probable cause to believe that a certain person listed in the subject block for committing an offense did or did not commit the offense.

7-7
Exceptions

The following are exceptions for listing individuals in the subject or victim sections of a ROI:

a. In accordance with paragraph 5-21d, CIDR 195-1, all death investigations will be conducted as though the death were a homicide until determined otherwise. Therefore, when an undetermined death, or a suspected justifiable homicide, suicide, accidental death, or natural death is involved, the deceased person will be shown in the victim section and “none" will be entered in the subject section if no other offenses are involved. In accordance with paragraph 5-21e(1), CIDR 195-1, all equivocal deaths and apparent suicides or suspected suicides will be initially reported/listed as "undetermined death" until the facts surrounding the death can be established.

b. The U.S. Government will be listed as the victim for all offenses involving voluntary possession, use, or sale of controlled substances, and for all offenses involving sex crimes between consenting adults except adultery (e.g., U.S. Government, Fort Example, FL 33141 [False Swearing]) (See paragraph 5-25 for further guidance on APCSM). In cases of adultery, the spouse of the married participant will be listed as the victim, unless one participant is not in violation of any law and the other participant (U.S. service member) is not married. In the latter case, the U.S. Government will be listed as the victim.

c. Corporate subject listing. A corporation is criminally liable for the acts of its agents, if the agent commits a crime within the scope of his employment and with intent to benefit the corporation.

d. Juveniles:

(1) Subjects. As with other civilian offenders, listing juveniles as subjects in a ROI is appropriate only if their activities are a violation of applicable federal, state and foreign statute. Juvenile offenders should be listed by name, followed by the automated ACIRS notation "JUVENILE-THIS RECORD MAY BE RELEASED ONLY IN ACCORDANCE WITH 18 USC, Section 5038(a)" entered at the end of the subject data. Paragraph 5-4b describes the investigative procedures for offenses committed by juveniles. 18 USC 5038 prohibits disclosure, directly or indirectly, of information contained in the ROI to anyone outside the investigating agency other than the judge, counsel, the U.S. Government, or other activities entitled to receive juvenile records. In overseas areas, if no U.S. statute with extraterritorial application has been violated and the host country law establishes a threshold age for criminality, those below the requisite age will not be listed in the subject block, but will be identified in the investigative summary of the ROI.

(2) Victims. Juvenile victims will be listed by name, followed by the automated ACIRS notation "JUVENILE - THIS RECORD MAY BE RELEASED ONLY AS AUTHORIZED BY AR 195-2, PARAGRAPH 4-3f” entered at the end of the victim data. AR 195-2 limits the distribution of ROIs involving juvenile victims to persons authorized access to juvenile offender records, those in normal distribution channels, and other law enforcement agencies when there are indications of criminal activity which may fall within the investigative responsibility of that

agency. Normal distribution of ROIs involving juvenile victims will be strictly limited to those with a need to know.

7-8
Lesser related offenses.

Persons who are found to be responsible for only administrative deficiencies or acts of neglect, not criminal in nature, will not be listed as a subject of a ROI. These incidents will be called to the action commander's attention in the investigative summary of the ROI or referred to the commander by written memorandum.

7-9
Lesser related offenses perpetrated by a listed subject.

Persons listed in a ROI for criminal offenses who, during the course of the investigation, are found to also have committed offenses that fall within those acts described in paragraph 7-8, will not be further listed for these acts or omissions. These incidents will be called to the action commander's attention in the investigative summary of the ROI or referred to the commander by written memorandum.

7-10
SSI reporting criteria

a. The SSI is designed to provide prompt notification to the CG, USACIDC and other designated recipients of any incident of alleged or actual criminal conduct which may cause unfavorable publicity for the Army, impact on the operational mission of USACIDC, or result in inquiries being directed to the CG, USACIDC. In cases of extreme seriousness or sensitivity, prompt telephonic notification to Current Operations, DCSOPS, HQUSACIDC (normal duty hours) or the HQUSACIDC Staff Duty Officer (non-duty hours) is required. Follow-up documentation will be provided to Current Operations.

b. The SSI (ONLY) or ROI/SSI report, as appropriate, will be submitted on incidents falling within the criteria described below:

(1) Threats, confrontations or information on other matters adversely affecting the personal security of the following personnel (immediate telephonic notification required):

(a) The Secretary of Defense.

(b) The Deputy Secretary of Defense.

(c) The Secretary of the Army.

(d) The Under Secretary of the Army.

(e) The Chief of Staff Army.

(f) The Vice Chief of Staff Army.

(g) Senior officials for which the USACIDC has responsibility for providing personal protection.

(h) Others designated by the CG, USACIDC.

(2) Terrorist acts directed against Army personnel or facilities and in overseas areas, any such act directed against any Army member or family member, DA civilian employee or family member, or Army equipment, materiel, or facility, within the geographic area of responsibility of the USACIDC. The USACIDC will also report such incidents directed against personnel and facilities of other services when located on or near Army installations (immediate telephonic notification is required).

(3) Incidents involving the non-training discharge of firearms by USACIDC personnel (attached or assigned) supporting USACIDC operations. All shooting incidents, including training, qualification, etc., by the above categories of personnel which result in death or injury will be reported (immediate telephonic notification is required).

(4) All incidents resulting in the death or serious injury of USACIDC personnel (attached or assigned) supporting USACIDC operations, unless such incidents result in minor injury, were accidental and not in connection with police operations (telephonic notification to reach HQUSACIDC within 4 hours).

(5) Incidents involving the actual or possible disclosure of classified information or the theft or deliberate destruction of classified material (Secret or higher), when CID is involved in some aspect of the investigation. Information about such incidents will be properly classified and transmitted by secure means, promptly reported to local military intelligence, and must be reported by HQUSACIDC to the Assistant Chief of Staff for Intelligence (DAMI-CI).

(6) Murder, voluntary manslaughter, assault with intent to commit murder, unattended deaths (less hospice deaths unless rank/grade is an issue), fatal traffic accidents, and suspected/confirmed self-inflicted deaths on or off post by active duty personnel, their family members or DA civilian employees.

(7) Rape, forcible sodomy, indecent assault, carnal knowledge, or indecent acts upon a child under 16 years of age.

(8) Kidnapping.

(9) The robbery of an activity or facility on an Army installation.

(10) Any incident under USACIDC purview that, as a result of conflict or mission, is categorized as a “war crime”.

(11) Larceny of U.S. Government property, funds, or frauds in excess of $50,000.00 (unless sub-paragraph 28 below applies).

(12) All aggravated arsons. All simple arson resulting in property damage in excess of $50,000.00.

(13) Lost, missing, or stolen U.S. Government arms, ammunition and explosives (AA&E), including Army ROTC, National Guard and Reserve units, in the following quantities:

(a) One or more missile or rocket rounds.

(b) One or more firearms (i.e., machine guns, automatic/semiautomatic fire weapons, manually operated weapons).

(c) Ammunition:

1. 50 caliber and smaller - 1,000 rounds or more.

2. Larger than 50 caliber - 5 rounds or more.

(d) Any fragmentation, concussion, or explosive grenade, to include artillery or ground burst simulators, or other type of simulator or device containing explosive materials.

(e) One or more mines (anti-personnel and antitank).

(f) Any demolition explosives, detonation cord, fuse, or other types of explosive materials.

(g) Any evidence of trafficking in AA&E, such as bartering for narcotics or any other thing of value, to include taking AA&E across international borders, regardless of the quantity involved.

(14) Offenses involving controlled substances in the following amounts:

(a) Marihuana 1,000 grams or more.

(b) Hashish 1,000 grams or more.

(c) Heroin 100 grams or more.

(d) Cocaine 100 grams or more.

(e) Methamphetamines 100 grams or more.

(f) LSD 100 or more dosage units.

(g) PCP 100 grams or more.

(h) Other controlled substances (amphetamines, barbiturates, other hallucinogens) in amounts of 100 gram/dosage units or more.

(15) Currency violations in excess of $10,000.00.

(16) Acts by groups of soldiers which constitute gross defiance of authority.

(17) Bribery, graft, and the illegal acceptance of gratuities in excess of $50,000.00.

(18) Conspiracies or attempts to commit any offense listed in (1) through (17) above.

(19) Any unauthorized root level access into an Army interest computer or network system (as defined in Chapter 12) where there is evidence of critical component manipulation and/or any access into a classified system. Root (or administrator) level access is defined as a level of access which, if attained, would allow system administration privileges and access rights beyond those of a routine user. A critical component is defined as a security router, Domain Named Server (DNS), domain server, or any computer responsible for the management of such components.

(20) All violations of AR 190-53 (wiretap, etc.) by personnel assigned to or working with the USACIDC. The requirement is in addition to the requirement to notify the military police (MP) for serious incident report (SIR) purposes (see AR 190-40).

(21) Child abuse in an Army organizational setting/facility or within an Army sponsored/sanctioned activity. This includes actual or alleged incidents of child abuse (i.e., physical abuse, sexual abuse or neglect) which take place within an organizational setting/facility (e.g., child development center, medical treatment facility, gymnasium, etc.) or an Army sponsored/sanctioned activity (e.g., youth

sport/recreation activity, field trips, etc.). This paragraph does not apply to incidents of child abuse occurring within the family unit.

(22) Any offense investigated by the USACIDC where a commander (any rank), a field grade commissioned officer (05 or above), a senior warrant officer (W4 or above), a senior noncommissioned officer (E8 or above), a senior DA civilian (GS14 or above), or a USACIDC special agent (present or former) is identified as a suspect or subject.

(23) If a senior person (see paragraph 5-4a) or a USACIDC special agent is involved as a suspect or subject, Current Operations, DCSOPS, HQUSACIDC, will be contacted telephonically prior to dispatch of the SSI and fully apprised of the facts. The HQUSACIDC will determine the appropriate mode in which to dispatch the SSI.

(24) If a Judge Advocate General Corps (JAGC) officer is involved as a suspect or subject for offenses related to the official duties as specified in paragraph 4-9b(1), DCSOPS, HQUSACIDC will be contacted telephonically prior to dispatch of the SSI and fully apprised of the facts. The HQUSACIDC will determine the appropriate mode in which to dispatch the SSI.

(25) Crime(s) under USACIDC investigative purview that pertain to the duties of a health care provider (see paragraph 4-31).

(26) Any incident/allegation regarding defective products or product substitution in which a serious hazard to health, safety, or operational readiness is indicated, regardless of the loss value.

(27) Any Incident/allegation of espionage, sabotage, aiding the enemy, or spying.

(28) Any incident/allegation investigated by MPFU involving a defense contractor with an estimated loss of 1 million dollars or more, or if the incident/allegation, regardless of dollar value, involves:

(a) a serious hazard to health, safety or operational readiness, or

(b) a Program Manager as a suspect, or

(c) Senior personnel as defined in paragraph 5-4 of this regulation, or

(d) Classified material or information.

(29) All incidents under USACIDC investigative purview involving a firearm used in the actual commission of the crime in which the firearm was used as a

means of threatened or actual deadly force. If this information is not immediately known, it will be included in subsequent report(s).

(30) Any incident investigated by USACIDC, which was determined to involve a hate crime.

(31) Missing Persons (ALCID 004-03)

c. The following information is to be reported directly to the U.S. Secret Service (USSS) by the fastest available means:

(1) Any information, whether it concerns immediate and present danger or past incident bearing on the personal security of anyone under the protection of the Secret Service. This information can be a threat, plan or attempt to physically harm or kidnap any of the following individuals:

(a) The President, the Vice President (or other officer next in the order of succession to the Office of the President), the President-elect, and the Vice President-elect.

(b) The immediate families of those individuals listed in paragraph (a).

(c) Former Presidents and their spouses for their lifetime, except that protection of a spouse shall terminate in the event of remarriage.

(d) Children of a former President who are under 16 years of age.

(e) Visiting heads of foreign states or foreign governments.

(f) Other distinguished visitors to the U.S. and official representatives of the U.S. performing special missions abroad when the President directs that such protection be provided.

(g) Major Presidential and Vice Presidential and, within 120 days of the general election, the spouses of such nominees/candidates.

(h) Foreign diplomatic missions located in the metropolitan D.C. area (and others as specified under statutes).

(2) The USSS solicits our responsiveness to the below stated guidelines regarding the prompt dissemination of this information:

(a) Information pertaining to a threat, plan, or attempt by an individual, group, or organization to harm physically or kidnap the persons protected by the USSS or any other high government officials.

(b) Information pertaining to threats, incidents, or demonstrations against foreign diplomatic missions (embassies, chanceries, and consulates).

(c) Information pertaining to individuals, groups, or organizations who have plotted, attempted or carried out assassinations or kidnapping of U.S. or foreign senior government officials.

(d) Information concerning the use of bodily harm, assassination, or kidnapping as a political weapon (this should include training and techniques used to carry out the act).

(e) Information pertaining to persons who insist upon personally contacting high government officials for redress of imaginary grievances, etc.

(f) Information pertaining to any persons who make oral or written statements about high government officials in the following categories:

1. Threatening statements.

2. Irrational statements.

3. Statements expressing unusual interest/fixation.

(g) Information pertaining to terrorists (individuals, groups) and their plans, capabilities and activities (bombings, etc.).

(h) Information pertaining to the ownership or concealment by individuals or groups of caches of firearms, explosives, or other implements of war when it is believed that their intended use is for other than legal purposes.

(i) Information pertaining to individuals who are perceived to be acting irrationally in their effort to make personal contact with high government officials; information concerning anti-American or anti-U.S. Government demonstrations abroad; information concerning anti-American, anti-U.S. Government demonstrations in the U.S. involving serious bodily injury or destruction of property; an attempt, or credible threat, to commit such acts in order to further political, social, or economic goals by said intimidating and coercive tactics.

(j) Information regarding civil disturbances.

(3) The USSS does not desire or solicit information pertaining to individuals or groups expressing legitimate criticism of, or political opposition to, the policies and decisions of the U.S. Government or its officials.

(4) A USACIDC unit will make immediate telephonic notification to HQUSACIDC subsequent to notifying the USSS on any of the foregoing listed information.

d. This list of SSI reportable incidents is not all-inclusive and any significant incident may be reported to HQUSACIDC, if deemed appropriate by the CID supervisor, especially if the incident is known to be of current interest to HQUSACIDC or HQDA.

7-11
SSI preparation and dispatch

a. The SSI reports, whether combined with a ROI or not, will be prepared in the same format as initial, status and, when applicable, supplemental ROIs.

b. The SSI reports may be submitted when the incident is not within the investigative responsibility of USACIDC. SSI reports, which are not combined with an ROI, will be referred to as a "SSI (ONLY)" report within USACIDC channels. When USACIDC has investigative responsibility, the SSI will be combined with the ROI.

EXAMPLE
SUBJECT: CID REPORT - INITIAL / SSI - 0015-99-CID000-00010-5H1B

c. SSI reports will be dispatched by COB of the first business day following notification to a USACIDC unit of an incident that meets the SSI criteria. Fragmentary information will be submitted, when full details are not known. Dispatch will not be delayed pending receipt of additional information.

d. The SSI reports will be dispatched by message, priority precedence or by ACIRS. When the transmission by electrical message might compromise the effectiveness of personnel concerned, or impede investigative activity, dispatch may be accomplished by telecopier, back channel message, or similarly secure means of communication.

e. In all death cases in which a CID investigation is initiated, the name and telephone number of the USACIDC casualty liaison officer (CLO) will be included in the SSI messages. (See paragraph 5-2l).

EXAMPLE
THE CASUALTY LIAISON OFFICER (CLO) FOR THIS OFFICE IS CW3 BURTIS REDFERN, SPECIAL AGENT-IN-CHARGE, AT DSN: 635-8510 OR COM: (540) 659-8510.

f. See chapter 8 for distribution of SSI ROIs.

7-12
Initial ROI

An initial ROI is a report dispatched to advise concerned commanders, CID supervisors, and other designated recipients that a USACIDC investigation has been initiated. (See figure 7-1).

a. An initial ROI will be dispatched by the close of business (COB) of the fifth business day following a determination that credible information exists that an offense has been committed which falls within USACIDC investigative responsibility.

b. See chapter 8 for distribution of initial ROIs.

c. Initial ROIs are dispatched using ACIRS or on DD Form 173 in accordance with AR 105-31. Initial ROIs will be dispatched by routine precedence and are prepared using all upper case characters.

d. Initial ROIs will be addressed to DIR, USACRC, USACIDC, ATTN: CICR-ZA. Additional authorized recipients of USACIDC ROIs identified in chapter 8 will be listed as information addressees.

e. When the initial ROI contains SSI reportable information, paragraph 7-10(a) and 11 will also apply.

f. Initial ROIs will be marked "FOR OFFICIAL USE ONLY" or classified as appropriate. ACIRS or similar non-secure systems will not be used to transmit classified information, CONFIDENTIAL or higher.

g. The subject line of the initial ROI will be identified as "SUBJECT: CID REPORT - INITIAL", the ROI number, and all offense codes.

EXAMPLE

SUBJECT: CID REPORT - INITIAL - 0015-99-CID000-00010-5H1B

If the incident is Defense Investigative Management Information System (DIMIS) or Violent Criminal Apprehension Program (VICAP) reportable it will be so indicated following the last offense code.

EXAMPLE

SUBJECT: CID REPORT - INITIAL - 0015-99-CID000-00010-5H1B (DIMIS)

EXAMPLE

SUBJECT: CID REPORT - INITIAL - 0015-99-CID000-00010-5H1B (VICAP)

h. Paragraph 1, DATES/TIMES/LOCATION OF OCCURRENCES. Enter the date, time, and location of occurrence of the incident originally reported to the USACIDC. The entry "Unknown" is not acceptable, as a reasonable estimate of time can nearly always be made. If only the year is known and the date cannot be determined, enter for example, 1 JAN 1998/0001 – 31 DEC 1998/2400. In cases involving multiple offenses occurring on multiple dates, times, and locations, reflect additional dates, times, and locations as separate entries.

i. Paragraph 2, DATE/TIME REPORTED. Enter the date and time when the incident was initially reported to the USACIDC. Significant delays between the time reported and the initiation of a ROI should be explained in the investigative summary. For example, the initial report might be submitted many days or weeks after the receipt of information that initially resulted in a preliminary investigation conducted under a sequence number. In this case, the delay between the initial receipt of information and the dispatch of the initial ROI should be explained in the investigative summary.

j. Paragraph 3, INVESTIGATED BY: Enter the name and sequence number of the special agent(s) responsible for the conduct of the investigation. The names(s) non-USACIDC investigative personnel (i.e., MP Investigators, local national investigators, etc) assigned to assist in the investigation will not be added to the ACIRS generated report in conjunction with the primary case agent. The name(s) of non-USACIDC investigative personnel assisting in the conduct of the investigation will be mentioned and fully identified elsewhere in the ROI (AIR, statement, etc).

k. Paragraph 4, SUBJECT. Enter as much of the following data as is known for each identified subject. Each subject entry, to include "Unknown", in the report will be automatically numbered by the ACIRS in sequential order:

(1) Last, first, and middle name.

(2) Military rank, civilian pay grade, or status.

(3) Nationality (if other than a U.S.).

(4) Social Security Account Number (SSAN).

(5) Date of birth.

(6) Place of birth.

(7) Sex.

(8) Race.

(9) Organization or address (DoD civilian employees, show employing organization).

(10) Major Command Activity Code (MCAC).

(11) Aliases or other names used.

(12) Former service numbers.

(13) If family members of military personnel or DoD civilian employees are subjects, the following sponsor identification data will be provided in parentheses immediately following the family member's identification:

(a) Family member relationship.

(b) Military rank or civilian pay grade.

(c) First, middle, and last name.

(d) Sex.

(e) SSAN.

(f) Organization or address.

(g) MCAC.

(14) Offenses pertaining to the individual.

(15) When a subject is identified and there is credible information (See paragraph 4-9a(1)) then the individual will be entered into the subject block. When there is an identified suspect and there is not credible information to enter the individual into the subject block, enter

/Link2 1585 0 R/Rect[0 0 0 0]/Subtype/Link/Type/Annot>>BT 1 0 0 1 0 0 Tm /F1 9 Tf 7.1 0 0 7.1 UT*(, U

(6) When distribution of the ROI is restricted in accordance with the provisions of AR 195-2 and paragraph 8-2b of the regulation, an additional paragraph will be used to document the reason for restricting distribution. This paragraph will be the first paragraph of the investigative summary, titled “RESTRICTED DISTRIBUTION” and will document the reason(s) for the distribution restriction (e.g., “RESTRICTED DISTRIBUTION: Due to the covert nature of this investigation, distribution of this report is restricted to USACIDC channels only”). All subsequent status/supplemental reports will contain this paragraph, until the distribution restriction is no longer required at which time a status/supplemental report will be initiated lifting the restricted distribution (e.g., "RESTRICTED DISTRIBUTION: Distribution of this report is no longer restricted to USACIDC channels."). See paragraph 7-13d(9).

EXAMPLE OF INITIAL ROI

6. INVESTIGATIVE SUMMARY: THE INFORMATION IN THIS REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY CHANGE PRIOR TO THE COMPLETION OF THE INVESTIGATION.

THIS INVESTIGATION WAS INITIATED UPON NOTIFICATION BY A USACIDC SOURCE THAT SGT SMITH HAD SOLD THE SOURCE APPROXIMATELY ONE OUNCE OF MARIHUANA FOR $75.00 IN U.S. GOVERNMENT FUNDS (.0015).

RESTRICTED DISTRIBUTION: DUE TO THE COVERT NATURE OF THIS INVESTIGATION, DISTRIBUTION OF THIS REPORT IS RESTRICTED TO USACIDC CHANNELS ONLY.

EXAMPLE OF STATUS ROI

6. INVESTIGATIVE SUMMARY: THE INFORMATION IN THIS REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY CHANGE PRIOR TO THE COMPLETION OF THE INVESTIGATION.

RESTRICTED DISTRIBUTION: DISTRIBUTION OF THIS REPORT IS NO LONGER RESTRICTED TO USACIDC CHANNELS.

2D STATUS:

THIS STATUS REPORT ….

(7) The decision to restrict distribution of a USACIDC report can include a variety of operational considerations such as:

(a) Minimizing the potential for harm of a covert agent, investigator, or source;

(b) Preventing compromise of a covert investigation;

(c) Preventing possible destruction of evidence;

(d) Preventing the flight of a suspect or subject; or

(e) Other considerations as determined by USACIDC supervisory personnel.

n. Paragraph 8. USACRC Criminal History Record Check. When USACRC criminal history record checks are required of subjects or victims listed in an initial ROI or added in a status ROI, list the name of the individual with a brief statement requesting the check (i.e., REQUEST NAME CHECK OF TOM JONES, PAUL SMITH, AND TAMMY FRENCH). If no checks are required this paragraph may be omitted.

o. Paragraph 9 (or 8). Suspension of favorable personnel actions/security clearances. In known subject cases involving Army members or DoD civilian employees who are listed for criminal offenses, commanders will be reminded of their responsibilities to suspend security clearances and favorable personnel actions. In these cases, the following will be automatically entered by ACIRS as the next-to-last paragraph: “COMMANDERS ARE REMINDED OF THE PROVISIONS OF AR 600-8-2 PERTAINING TO SUSPENSION OF FAVORABLE PERSONNEL ACTIONS AND AR 380-67 FOR THE SUSPENSION OF SECURITY CLEARANCES OF PERSONS UNDER INVESTIGATION.” There is no requirement to include this paragraph on reports where the subject is unknown, deceased, or a non-DoD civilian, when there are no subject changes, or on reports which delete subjects.

p. Paragraph 10 (or 9). The final paragraph will state that USACIDC reports are exempt from automatic termination of protective markings in accordance with Chapter 3, AR 25-55. This entry will not be used if the report contains classified defense information (CONFIDENTIAL or higher); in such cases, appropriate downgrading instructions will be provided in this paragraph.

7-13
Status ROI

A status ROI is a report submitted to provide information on significant developments during the course of an investigation or to correct previously reported information. The status ROI reflects the overall conduct of the investigation and may include information on the administration of the case such

as pending leads, laboratory examinations and investigative methodology. (See figure 7-2).

a. Status ROIs are prepared in similar format as the initial ROI. Status reports are submitted only when the development of new information warrants providing an update on a case, and must contain enough information to articulate the progress of the investigation. Normally, this will be accomplished by repeating pertinent information on dates, times, locations, individuals involved. When previously reported information needs to be changed, the correct information will be reported in the appropriate paragraph of the report and the reason for the change discussed in the investigative summary.

b. Paragraph 6, INVESTIGATIVE SUMMARY. As with initial ROIs, the first paragraph of the investigative summary will read as follows: “THE INFORMATION IN THIS REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY BE CHANGED PRIOR TO THE COMPLETION OF THE INVESTIGATION." Immediately following, a second paragraph will be used to identify the type of report submitted (e.g., 2D STATUS, 3D STATUS, etc.) and the reason for submission. The third paragraph of the investigative summary will also present a brief description of the incident, answering the basic questions of who did what to whom; when, where, and how it was done, and, if known, why. The basic elements of proof for each offense cited will be established when writing the investigative summary. Dates, times, and locations for all additional incidents being reported will be presented to clarify the sequence of events for the reader.

EXAMPLE

2D STATUS:

THIS STATUS REPORT IDENTIFIES TWO SUBJECTS OF THIS INVESTIGATION AS DETERMINED FROM A SWORN STATEMENT BY SGT RONALD J. JACKSON, 595-59-5999, COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22606; CORRECTS THE TIME OF OCCURRENCE BASED ON THE WITNESS' STATEMENT; UNFOUNDS THE OFFENSE OF HOUSEBREAKING; ADDS THE OFFENSE OF CONSPIRACY AND CORRECTS THE SSN OF VICTIM NUMBER 1 (SPC SMITH).

SGT JACKSON WAS INTERVIEWED AT 1145, 2 NOV 98, AS PART OF A CANVASS INTERVIEW OF BUILDING 101 OCCUPANTS. SGT JACKSON, WHO RESIDES IN ROOM 313 ADJACENT TO THE VICTIM'S ROOM, WITNESSED SGT JONES AND SPC THOMPSON (ROOMMATES OF SPC SMITH) LOADING THE VICTIM'S TELEVISION SET ONTO THE REAR OF A PICKUP TRUCK BELONGING TO SGT JONES AT 2110, 30 OCT 98.

THE VICTIM STATED IN HIS SWORN STATEMENT, 31 OCT 98, THAT HE SUSPECTED SGT JONES BECAUSE SGT JONES WAS EXPERIENCING SIGNIFICANT FINANCIAL PROBLEMS.

SGT JONES AND SPC THOMPSON HAVE NOT BEEN INTERVIEWED, BECAUSE THEY ARE ON LEAVE UNTIL 23 NOV 98.

INITIAL REPORT:

(REPEAT INFORMATION APPEARING ON INITIAL REPORT)

c. Dispatch and distribution of the status ROI is the same as that described for an initial ROI. Status ROIs will be numbered sequentially, beginning with "2D STATUS."

d. In the preceding paragraphs, the time frame at which time the dispatch of a status ROI is required is established as COB of the fifth business day following the need for the report. Unless otherwise noted, this is a constant unless the report in question is SSI reportable (see paragraph 7-10). If SSI reportable, the time frame for dispatch will be by COB of the first business day following the need for the report. For clarification, a “business” day is any day that does not fall on a weekend, national holiday or HQUSACIDC approved training holiday. A status ROI is required:

(1) By COB of the fifth business day following the identification of a new subject.

(2) By COB of the fifth business day following the determination that a previously reported subject did not commit an alleged offense, that an offense is determined to be unfounded, or that a previously reported victim is not the victim of an alleged offense. The status ROI will not delete subjects or victims; however, the investigative summary will document the circumstances surrounding the determination that an individual is not a subject or victim, or that the offense is being unfounded.

(3) By COB of the fifth business day following receipt of information which changes the name, spelling of a name, or SSAN of any previously reported subject or victim.

(4) By COB of the fifth business day following receipt of information that a previously listed subject has been dropped from the rolls as a deserter. The status ROI will provide the date the deserter's unit forwarded the DA Form 4187 (Personnel Action) to the U.S. Army Deserter Information Point (USADIP).

(5) By COB of the fifth business day following assumption of investigative responsibility by another agency.

(6) By COB of the first business day following the agreement by a U.S. attorney to prosecute a command monitored or SSI reportable EC case. Declinations to prosecute such cases are handled in accordance with paragraph 4-15.

(7) By COB of the fifth business day following a determination that the ROI is DIMIS or VICAP reportable.

(8) If the investigation involves the use of a DoD Inspector General (DoDIG) subpoena duces tecum (DD Form 2287) and HQUSACIDC directs that status reports be submitted to meet requirements of the DoDIG.

(9) When ever the distribution of an initial or status report is limited to USACIDC channels only, a status ROI must be submitted to lift the restriction. Once restriction has been lifted, reinstatement can only be accomplished through coordination with the Office of the Director, USACRC.

EXAMPLE

6. INVESTIGATIVE SUMMARY: THE INFORMATION IN THIS REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY CHANGE PRIOR TO THE COMPLETION OF THE INVESTIGATION.

3D STATUS:

THIS STATUS REPORT IS BEING SUBMITTED TO RESCIND PREVIOUS RESTRICTIONS TO THE DISSEMINATION OF THIS REPORT OUTSIDE USACIDC REPORTING CHANNELS.

(10) When, in the opinion of the case agent or CID supervisor, there are significant new developments in the cases which warrant reporting to all recipients of the status ROI. Examples might include citation of significantly more serious offenses (e.g., attempted murder to murder, recovery of sensitive property, etc.).

e. Status ROI and message supplemental ROIs (see paragraph 7-17) are the only authorized means of adding or deleting subjects and victims. In those rare instances when a decision is made to change subject or victim information at the time of final ROI preparation, a status report with the appropriate changes will be dispatched prior to the final ROI.

f. Identified subjects and victims will not be renumbered. Once assigned, a number will remain associated with the subject or victim throughout the investigation. "Unknown” subjects or victims will be identified by submission of a status report correcting (updating) the previously unknown identity. Subjects or victims of ROIs may only be deleted as authorized by paragraph 7-4, or as otherwise directed by HQUSACIDC. The reasons for these changes will be explained in the investigative summary. If either a subject or victim is deleted, the number originally assigned will be carried forward on all subsequent reports with the notation "Previously Deleted" automatically entered by the ACIRS.

g. A status ROI is not required, when the purpose is to “ADD” or “DELETE” a cited offense. In such instances, the new offense information is entered following the subject and victim identification blocks.

7-14
Final ROI

A final ROI is submitted at the conclusion of investigative activity. The final ROI will be prepared in the format and order specified below. Line spacing and format of front page are mostly ACIRS generated and follows standard Army memorandum format. Normal capitalization will be used throughout, except that family names will be all uppercase. (See figure 7-3).

a. See chapter 4 for final (C) and final (D) ROI criteria.

b. See chapter 8 for distribution of final ROIs.

c. After MEMORANDUM FOR SEE DISTRIBUTION, the "SUBJECT:" will be followed by "CID REPORT OF INVESTIGATION," a hyphen, "FINAL," a hyphen and the report number followed by offense codes. If DIMIS and VICAP reportable, this will be indicated within parentheses following the last offense code.

d. The DATES/TIMES/LOCATIONS OF OCCURRENCES information is entered in the same manner as for initial ROIs.

e. The DATE/TIME REPORTED information is entered in the same manner as for initial ROI.

f. The INVESTIGATED BY information is entered in the same manner as for initial ROIs.

g. SUBJECT and VICTIM.

(1) These sections will identify subjects and victims in the format specified for initial ROIs; however, the MCAC will not be included. The format and exclusion of the MCAC is controlled by the ACIRS. Particular care must be taken; however, to ensure that subjects are cited for violations of laws to which they are subject to. As an example, civilians not subject to the UCMJ and cannot be listed as subjects of purely military offenses such as violation of a lawful general order or regulation.

(2) Each subject and victim listed in the final ROI will be numbered sequentially. The number assigned to a particular subject or victim in a final ROI will also be used in any supplemental ROI. "Unknown", "None," and “Not Applicable” entries will also be numbered. "None" entries will be used only when all offenses are unfounded and no person or entity (including "Unknown") is listed for any offense.

(3) Additions and deletions, before dispatch of a final ROI, will be accomplished only by status ROI. Once dispatched, additions or deletions to a final ROI can only be accomplished through a message supplemental ROI. The final ROI will not contain "ADD" or "DELETE" entries.

h. INVESTIGATIVE SUMMARY. The investigative summary of the report will be a concise summation of the results of the investigation and answer, in concert with other sections of the report, the questions of who, what, when, where, how, and why, if known. The summary, in separate paragraphs, first documents the background that lead to the initiation of the investigation (basis for investigation) and then a synopsis of the investigative conclusions reached (probable cause statement). The report’s statutes, exhibit/substantiation and investigative/prosecutive status sections then support the investigative conclusions. The end of the ROI will identify the preparer, approver, and appropriate distribution.

(1) Basis for investigation. This paragraph of the investigative summary will present a brief description of how the allegation under investigation was initially reported to the investigating USACIDC unit. This description will include, as a minimum, how the incident was first brought to the attention of law enforcement, who reported the incident to the reporting USACIDC unit, and what was initially reported.

(2) Probable cause statement. This paragraph will contain a brief description of the incident. In concert with other parts of the ROI, the basic questions of who, what, when, where, how, and why, if known, should be answered about each offense and/or incident. Allegations of criminal activity originally reported and investigated, but determined to be unfounded will also be discussed. Unnecessary detail such as serial numbers, license plate numbers, colors, makes, and models of property, will not normally be included in the investigative summary of the final ROI unless relevant to the investigation. However, elements of proof, to include the total consolidated property values, segregated by

government and/or private property, must be reported in the investigative summary. Criminal cost avoidance may also be included if such information is meaningful, justifiable, easily understood and applicable. Specific language and/or terminology may be incorporated in the investigative summary as follows:

EXAMPLE

(1) Investigation established probable cause to believe that ...

(2) Investigation established that the offense of ... did not occur as alleged.

(3) Investigation revealed that ... did not commit the offense of ... as alleged.

(4) Investigation established there was insufficient evidence to determine ...

EXAMPLE

INVESTIGATIVE SUMMARY: On 10 Jan 99, SGT ARLINGTON reported that while jogging down Sunset Road, Fort Example, FL, she was approached by SGT JOHNSON. SGT ARLINGTON added that while sitting in SGT JOHNSON's vehicle and engaged in conversation, he physically forced her into the back seat of the vehicle, and raped her. SGT JOHNSON then drove SGT ARLINGTON to her residence, where she subsequently reported the incident to the military police.

Investigation determined that SGT JOHNSON did not commit the offense of rape, as originally reported by SGT ARLINGTON. Investigation did establish probable cause to believe that SGT ARLINGTON committed the offense of False Swearing when she, after falsely reporting she had been raped by SGT JOHNSON, rendered a sworn statement she knew to be false.

EXAMPLE

INVESTIGATIVE SUMMARY: On 10 Jan 99, the Commander, A Co, 71st Ord Bn, Fort Example, FL, reported that SGT JOHNSON had been identified as a drug offender through the conduct of a command directed urinalysis conducted on 25 Dec 98.

Investigation established probable cause to believe that SGT JOHNSON committed the offense of Wrongful Use of a Controlled Substance. During a command directed urinalysis, SGT JOHNSON submitted a urine sample which was subsequently tested and found positive for the presence of cocaine.

EXAMPLE

INVESTIGATIVE SUMMARY:

On 10 Jan 99, a USACIDC source reported that WMNV, a sub-contractor for

DYNCORP, was over-charging the U.S. Government for refuse collection services.

Investigation established probable cause to believe that WMNV committed the offense of False Statements and False Claims when the sub-contractor knowingly submitted claims requesting payments for the collection and disposal of refuse which they knew to be wrongfully inflated by $25,235.95.

Criminal Cost Avoidance:

One-Time: $25,235.95
Annual: Not Applicable

EXAMPLE

INVESTIGATIVE SUMMARY: On 10 Jan 99, the Fort Example Military Police reported that SGT JONES's chain-of-command had reported that SGT JONES had alleged having been raped by SPC SMITH.

Investigation did not develop sufficient evidence to prove or disprove SGT JONES' allegation that SPC SMITH raped her. SGT JONES reported that SPC SMITH, after returning to their barracks from the NCO club, forced her into her barracks room and raped her. SPC SMITH denied he raped SGT JONES, stating the act of sexual intercourse was consensual. Subsequent investigation did not identify any witnesses to the incident and SGT JONES' delay in reporting the incident negated the potential value of any physical evidence. Further investigation did not diminish the integrity or credibility of SGT JONES' allegation.

Additionally, when identifying and listing multiple incidents, attention must be taken to be brief and concise, avoiding excessive duplication of previously reported information.

(3) Statutes paragraph. The citation will list the applicable sections of the UCMJ, USC, state criminal code, or foreign statutes, which have been violated as supported by the investigation. This section will also be to identify offenses which were investigated and unfounded. In these cases, the statutes which were originally reported as having been violated will be listed, followed by the word "unfounded" in parentheses.

EXAMPLE

INVESTIGATIVE SUMMARY:

STATUTES:

Article 134, UCMJ: False swearing.

Article 125, UCMJ: Sodomy, consensual.

Article 120, UCMJ: Rape (unfounded).

Title 18, USC, Section 2031: Rape.

18.2 Section 67.2, Criminal Code of Virginia: Rape.

(4) Exhibits/Substantiation. Exhibits will be listed numerically in two separate sections entitled "ATTACHED" and "NOT ATTACHED." The substantiation provides a brief description of the exhibit in question and documents, through its description, how the investigative conclusions were reached. Items that were obtained in connection with the investigation, but were subsequently determined to possess no pertinence or evidential value will not be listed.

EXAMPLE

EXHIBITS/SUBSTANTIATION:

ATTACHED:

NOT ATTACHED:

(a) Exhibits will be listed numerically and with a brief description of the contents of the exhibit itself. In preparing the brief description, information should be included that clearly highlights significant events addressed by the exhibit(s), to include information that supplements the report's investigative conclusions.

(b) Attached. Exhibits or copies of exhibits that are attached to the report will be listed under this heading. Exhibits that are attached only to certain copies of the report will be identified with the distribution in parenthesis following the listing of the exhibit and will be placed towards the end of this section. Generally, any documentary-type evidence, which has been seized during the course of the investigation and would contribute to an understanding of the case or support the conclusions thereof, will be included under this heading. Items that are not informational in nature, such as handwriting exemplars, standards and documents collected for fingerprint evidence, will normally not be listed under this section.

1. Exhibits will be listed in chronological order, based on when they were prepared or collected. This order; however, is not applicable to the Agent’s Investigative Report (AIR). Since an individual AIR often documents numerous activities performed on numerous dates, the AIR should precede the exhibits it addresses. As an example, with an AIR that documents the crime scene processing, victim interview, and suspect interrogation, the exhibits following the AIR should be the crime scene sketch, victim’s statement, and suspect's waiver

certificate and statement, respectively. Using this methodology, the AIR serves as a "blue print" and aids in providing a logical structure to the presentation of attached exhibits.

EXAMPLE

ATTACHED:

1. Agent's Investigative Report (AIR) of SA HUDSON, 15 Jan 99, detailing his receipt of the initial complaint, crime scene processing, initial interview of SGT ARLINGTON, and interview of Dr. (LTC) ANDREWS.

2. Crime Scene Sketch, 10 Jan 99, prepared by SA MONTANO.

3. Sworn Statement of SGT ARLINGTON, 10 Jan 99, in which she related how she was confronted by SGT JOHNSON and forced to engage in sexual intercourse with him.

4. (4-1/4-2) Medical examination reports concerning SGT ARLINGTON and SGT JOHNSON, 10 Jan 99, detailing the lack of internal injuries to SGT ARLINGTON and the collection of sexual assault protocols from SGT ARLINGTON and SGT JOHNSON.

2. The investigating USACIDC unit will normally retain negatives (originals) of all photographs exposed during the investigation until all legal proceedings are completed. Photographic exhibits will be attached to all copies of the ROI retained within USACIDC channels, those forwarded to the Armed Forces Institute of Pathology (AFIP), and the supported SJA or prosecutor. High quality color prints of digital images are not routinely required as attachments for other than the file, USACRC, and AFIP copies, except if required to show something of evidential value. Prints produced using a laser or similar quality printer will routinely be used to create the copies needed as attachments to the ROI. Prints may be attached to other copies of the report as deemed appropriate.

3. Foreign language exhibits and their English translations will be listed as separate attached exhibits. Distribution of the foreign language exhibit will be limited to USACRC and file copies only. When foreign language exhibits are attached to the ROI, they will normally be mentioned in the AIR along with the full name of the person preparing the translation.

EXAMPLE

5. English language translation of Mr. ALVAREZ’s statement, Exhibit 16, translated by SA MONTANO.

X. (Other Exhibits)

16. Spanish language statement of Mr. ALVAREZ, 10 Jan 99, relating that he was the ground's keeper for Range Number 3 and that he did see two people by the wood line, but did not believe their encounter was confrontational (USACRC and file only).

EXAMPLE

At 1730, 10 Jan 99, Mr. Juan ALVAREZ, 100-00-1234, 7640 Carlyle Ave, #7b, Miami Beach, FL 33141, was interviewed by SA MONTANO, in his native language of Spanish. During his interview, Mr. ALVAREZ rendered a statement in which he related that he works as a contracted ground’s keeper assigned to Range 3. Mr. ALVAREZ stated that at around 0645, 10 Jan 99, he saw two people sitting in a dark Fort Explorer, however, he did not see any activities that would have suggested a confrontation between either person. (See translation of Mr. ALVAREZ's statement for details).

4. Certain exhibits are attached to a ROI, but are limited in their distribution. This includes photographic negatives, laboratory requests, evidence/custody documents, etc. In such cases, these exhibits should be listed towards the end of this section. For ease of reproduction, the same procedure should be used for bulky exhibits such as photographic packets, oversize documents, etc.

EXAMPLE

17. Photographic packet comprised of 37 photographs.

a. Packet containing photographs 1-20 (crime scene).

b. Packet containing photographs 21-37 (crime scene).

18. Compact disc 990001.101 containing all photographic images and the originals of Exhibit 17 (USACRC copy only).

19. Crime Lab Examination Request, 14 Jan 99, requesting that the clothing of both SGT ARLINGTON and SGT JOHNSON be examined to determine if either contained fluids which could determine if they engaged in sexual activities with each other (USACRC and file only).

20. (20-1 through 20-4) DA Form 4137, Evidence/Property Custody Document, vouchers (VO) 022-99, 023-99, 024-99 and 025-99, 11 Jan 99.

5. The case file number, including the ROI number, must be marked on each exhibit (e.g., 0000-01-CID000-00000). There is no requirement to annotate the primary offense code on any exhibit.

(c) Original documents required for subsequent administration of disciplinary action will be initially retained by the investigating USACIDC unit. Documents not required for this purpose will be attached to the original copy of the report being forwarded to USACRC. Original documents retained by the investigating USACIDC unit will be forwarded to USACRC, when no longer required. (See paragraph 7-32(g) for procedure).

(d) Photographic packets will be listed as a separate numbered exhibit. The negatives or original images will also be listed as a separate exhibit. If sub-packets are used, the report will reflect the number of sub-packets in the following manner, with the sub-packets marked accordingly.

EXAMPLE

15. Photographic packet comprised of 6 photographs (photographs 38-43). (Minor injuries of SGT ARLINGTON).

16. Photographic negatives (originals) of Exhibit 15 (USACRC only).

17. Photographic packet comprised of 37 photographs.

a. Packet containing photographs 1-20 (crime scene).

b. Packet containing photographs 21-37 (crime scene).

18. Compact disc 990001.101 containing all photographic images and the originals of Exhibit 17 (USACRC copy only).

(e) Not attached exhibits. Exhibits that are not attached to the report will be listed under this heading with subheadings to show their actual location or disposition. When applicable, these exhibit listings will include the name of its owner/person pertaining to in parenthesis and the item/voucher number.

EXAMPLE

NOT ATTACHED:

Retained in the evidence depository, this office:

28. Sexual assault protocol (SGT ARLINGTON), VO 022-99.

29. One pair of gray sweat pants (SGT ARLINGTON), VO 023-99.

Retained in the files of the U.S. Army Crime Records Center, Fort Belvoir, VA:

30. Polygraph authorization (SGT JOHNSON), 23 Feb 99.

31. Polygraph examination statement of consent (SGT JOHNSON), 24 Feb 99.

32. Four polygraph charts (SGT JOHNSON), 24 Feb 99.

(f) The location of all originals will be reported in a separate paragraph after the exhibits section. If the location of a particular exhibit is already known (e.g., photographic negatives (originals) of Exhibit 6 (USACRC copy only)) there is no need to restate where the original of this exhibit is retained. Unless they are Polaroid or other "instant" type, photographs are not "originals" in the sense of this paragraph; therefore, it is not necessary to record their disposition.

EXAMPLE

The originals of Exhibits 1 through 7, 9 through 12, and 14 are attached to the USACRC copy of this report. The original of Exhibits 8 and 13 are retained in the files of this office, pending adjudication. The original of Exhibit 19 is retained in the files of the U.S. Army Criminal Investigation Laboratory, Forrest Park, GA 30297-5122. The originals of Exhibit 20 are retained in the files of the evidence depository, this office.

(g). When performing analysis of electronic storage media (see Chapter 12), seized media such as hard drives are routinely forensically reproduced to separate media such as compact disks (CD), tapes, or other hard drives. In turn, these forensic reproductions are used to produce working copies of the seized media or as the “best evidence” available when the seized media must be returned prior to completion of the investigation. Unless warranted by special circumstances, such as discussed in paragraph 7-14h(4)(i), neither the seized media nor a forensic reproduction of the media will be forwarded to the USACRC as an attached exhibit to the Final ROI. When electronic storage media or a forensic reproduction of the media is retained as evidence, the Final ROI will reflect that evidence as “not attached,” with the location of the media under the heading of “Retained in the evidence depository, this office.” Further, when a forensic reproduction is made and used as a “working copy,” the location of this reproduction will be reflected as “not attached” evidence under the heading of “Retained in the case file pertaining to this investigation:”

EXAMPLE

NOT ATTACHED:

Retained in the evidence depository, this office:

15. One hard drive, model IBM-DALA-3540, serial number 1J90J281202 (SGT ARLINGTON), VO 025-01.

Retained in the case file pertaining to this investigation:

16. Five compact disks containing the “working copy” of Exhibit 15

(h) When performing electronic media analysis of the forensic reproduction or “working copies”, evidence and/or significant data discovered during the analysis should be copied to separate media (preferably CD). Unlike CDs used to store the seized media’s forensic reproduction, CDs used to store electronic evidence of a crime or significant data will be included in the Final ROI as an “attached” exhibit:

EXAMPLE

ATTACHED:

14. One compact disk containing various images and significant data extracted from Exhibit 16 (CRC copy only)

(i) When CDs or other exhibits containing data considered inappropriate for routine distribution (i.e., adult and child pornography, financial records, etc) are produced, these CDs or exhibits will only be attached to the USACRC copy of the ROI. For further information concerning prohibited images refer to paragraph 12-8, Chapter 12.

(5) Status paragraph. This section is used to record the status of the investigation at the time the report was terminated, action taken against offenders, or prosecutive decisions reached as a result of legal coordination.

(a) The status of the investigation and, when available, action taken against subjects will be reported for all ROIs. When action taken is reported, information provided will consist of a concise summary of the action taken. In the event the action commander takes action against the soldier for an offense other than the one(s) listed in the CID report (such as a lesser included offense), the revised offense will be specified. (ALCID 002-03)

EXAMPLE

INVESTIGATIVE SUMMARY:

STATUS: This is a final report. Commander's report of action (DA Form 4833) is pending.

EXAMPLE

INVESTIGATIVE SUMMARY:

STATUS: This is a final report. On 6 Mar 85, CPT John R. JONES, Commander, HHC, 71st Transportation Bn, reported that on 22 Feb 94, SP4 WILLIAMSON was administered non-judicial punishment under the provisions of Article 15, UCMJ. WILLIAMSON was reduced to PFC, ordered to forfeit $250.00 a month for two months, and to perform extra duty for 30 days. The reduction was suspended for 90 days.

(b) This section may also be used to report the prosecutive status of the case. This would normally be appropriate for those investigations referred to U.S. attorneys or to other federal, state or local jurisdictions for criminal prosecution, civil litigation, or administrative action. Recording this information partially satisfies the requirement by DoD and the Department of Justice (DOJ) to monitor the status of investigations after closure. In some cases this may create a Rule 6(e) disclosure problem; therefore, coordination should be effected with the responsible DOJ attorney before disclosure of prosecutive status.

EXAMPLE

STATUS: This is a final report. On 30 Jul 93, this case was discussed with Assistant U.S. Attorney John M. PATTON, U.S. Attorney's Office, District of Colorado, who indicated that his office would not seek prosecution because the amount involved was less than their $25,000.00 threshold limit.

EXAMPLE

STATUS: This is a final report. On 30 Mar 94, MAJ William K. LANTIS, office of the Staff Judge Advocate, Ft Blood, TX, was contacted. MAJ LANTIS said his office will recommend debarment of Mr. GROSS and the XYZ Pastry Corp.

EXAMPLE

STATUS: This is a final report. On 29 Mar 94, Assistant U.S. Attorney John M. PATTON, U.S. Attorney's Office, District of Colorado, stated that his office was seeking an indictment of Mr. GROSS and Mr. BRADY and the case would be presented to the grand jury on 15 Apr 94.

(c) If an investigation is terminated in accordance with the provisions of chapter 4, section V (Termination of Investigations), the basis for termination, including a citation of the applicable subparagraph, as well as a general summary of those investigative leads that will not be pursued, will be reported in the status section.

EXAMPLE

STATUS: This is a final (C) report. This investigation is being terminated in accordance with Section V, paragraph 4-17(6), CIDR 195-1, in that the special agent-in-charge has determined that furtherance of this investigation would be of little or no value and that leads remaining to be developed are not significant. Remaining leads include additional canvass interviews and USACIL examination of clothing seized. Commander's report of action (DA Form 4833) is pending.

EXAMPLE

STATUS: This is a final (C) report. This investigation is being terminated in accordance with Section V, paragraph 4-17(8), CIDR 195-1, in that a thorough investigation has failed to produce any logical subjects and there is no serious injury and/or substantial loss of government or personal property. Remaining leads include additional canvass interviews and continued review of local pawnshop receipts. Commander's report of action (DA Form 4833) is not required.

(6) Preparer and approver.

(a) The special agent or military police investigator who prepared the final ROI will sign the report. Type, on the second line below the last line of text, "Report Prepared By:" On the fifth line below the heading type, in all upper case, the name of the agent or investigator. The line below the name is the title (Special Agent or MP Investigator), followed by the agent's sequence number or investigator's credential number. The signature of the preparing agent/investigator indicates the report accurately reflects the investigative activity conducted, that it is investigatively complete, and has been prepared in accordance with pertinent regulations, other policy, and doctrine. If the preparer of the report (special agent only) is also the approving authority, the "Report Prepared By" entry is not required. If the agent/investigator is not available to sign the report in a reasonable period, another agent/investigator may sign the report for the preparing agent/investigator.

(b) The approving authority block is prepared in the same format and on the same lines as the preparer block. The approving authority must be a CID supervisor, as defined and approved by the local office or chain-of-command. The block is left justified to the center of the page. The approver's signature

indicates approval of the investigation, investigative techniques and procedures employed, and the content and format of the report. Enter in typed uppercase letters the name, rank, branch, and title of the approving authority. When the approver is a special agent, only the name and title need be entered. If desired; however, the special agent's rank and branch can be used.

EXAMPLE

STATUS: This is a final report. Commander's Report of Disciplinary Action Taken (DA Form 4833) is pending.

Report Prepared By:	Report Approved By:
KATHI L. HUDSON Special Agent, 3812	GUIDO CANDRELLA Special Agent in Charge
OR	
KATHI L. HUDSON Special Agent, 3812	GUIDO CANDRELLA CW2, MP Special Agent in Charge

(7) Distribution. List the recipients of the report and the number of copies provided to each. Specific identification of recipients will be recorded.

EXAMPLE

DISTRIBUTION:

1 - DIR, USACRC (original), Fort Belvoir, VA 22060
1 - Action Commander:
THRU: CDR, 71st Ord Bn, Fort Example, FL 33141
TO: CDR, A Co, 71st Ord Bn, Fort Example, FL 33141
1 -THRU:
CDR, 2nd MP Bn, USACIDC, Fort Standard, GA 22102
CDR, 3rd MP Group, USACIDC, Fort Gillem, GA 30297
TO: CDR, HQUSACIDC (ATTN: CIOP-CO), Fort Belvoir, VA 22060
1 - SJA (ATTN: CPT MITCHEM), Fort Example, FL 33141
1 - PMO (ATTN: MPR 00001-99), Fort Example, FL 33141 (e-mail)
1 - File

7-15
Initial/Final ROI

When an investigation can be initiated and completed in an expeditious manner, an Initial/Final ROI may be submitted instead of a separate initial and final ROI. Initial/Final ROIs will be prepared using the same format as a final ROI. An Initial/Final ROI is used to document the expeditious completion of an investigation in which circumstances allow for a final report to be dispatched within 5 business days. While intended primarily for non-SSI reportable offenses, an Initial/Final ROI may be used to document a SSI reportable incident. SSI reportable offenses may be documented as an Initial/Final (SSI), as long as circumstances allow for the report to be dispatched within current timeliness of reporting standards as prescribed by Chapter 7 and Appendix D of this regulation. An Initial/Final ROI would be appropriate, for example, to document the completion of a urinalysis or property crime investigation in which all appropriate investigative activities have been completed within the 5 business day period. (See figure 7-15).

a. After MEMORANDUM FOR SEE DISTRIBUTION, the "SUBJECT:" will be followed by "CID REPORT OF INVESTIGATION," a hyphen, "INITIAL/FINAL," a hyphen and the report number followed by offense codes. If terminated as a Final(C) ROI or reportable as a (DIMIS), ViCAP, or SSI incident, this will also be indicated within parentheses as further prescribed in this chapter.

b. All remaining paragraph requirements are identical to the requirements for a Final ROI, as further outlined in this chapter.

c. See chapter 4 for final (C) ROI criteria and guidelines.

d. See chapter 7 for DIMIS, ViCAP and SSI reporting criteria and guidelines.

e. See chapter 8 for distribution guidelines.

f: Initial/Final ROIs do not allow for the normal processing of criminal history checks for subjects and/or victims, or for the inclusion of those checks in the ROI. Results of criminal history records checks must be included in Initial/Final ROIs. If a criminal history check of a subject was conducted within the last 60 days, then an additional criminal history check is not required provided the previous history check is annotated in the current Initial/Final ROI. If appropriate, a NCIC check and a local provost marshal’s office check should be conducted. In order to complete and include the results of criminal history checks for Initial/Final ROIs

only, either a telephonic name check request made to USACRC or an electronic message request forwarded to the following ACIRS e-mail address will be used:

mailcicr@acirsf.belvoir.army.mil

This e-mail address will only be used for completion of Initial/Final ROIs.

7-16
Interim ROI

The interim ROI is a comprehensive packet documenting all investigative activity conducted through a specific date. It is comprised of a memorandum and copies of initial and/or status reports, statements, sketches, AIRs and other documents deemed pertinent by the CID supervisor releasing the information. The interim report is designed to serve as a vehicle for providing commanders, SJA, and other official recipients with information on the status of a particular investigation. The interim report provides the same information as would be reported in a final ROI, except that there are leads not yet accomplished. (See figure 7-4).

a. The subject line of the memorandum will be prepared as follows: "SUBJECT: CID Interim Report - 0001-99-CID000-00001 - (Offense Codes) (as of 1 Jun 99)." The "as of" date refers to the date of last investigative activity documented and will not necessarily be the same as the date of the report itself. The memorandum will also include, as a separate paragraph, a brief explanation as to its purpose and applicability.

EXAMPLE

MEMORANDUM FOR (Action Commander/Official)

SUBJECT: CID Interim Report - 0001-99-CID000-00001- 5L2B / 5L2C (as of 1 Jun 99)

1. The attached CID report(s) and supporting documents are forwarded for information and/or action as deemed appropriate.

b. The interim ROI is intended for the convenience of action recipients and need not be forwarded to USACRC or any other USACIDC element superior to the preparing office. When prepared, a copy of the memorandum will be maintained in the case file.

c. The memorandum will reflect, as a separate paragraph, that additional investigative activity will be conducted and reported and that findings may change. A reminder will also be included about the provisions of AR 600-8-2 and AR 380-67.

EXAMPLE

2. This is an interim report. Additional investigative activity will be conducted and documented in subsequent report(s). The information in this report is based upon an allegation or preliminary investigation and may change prior to the completion of the investigation. Commanders are reminded of the provisions of AR 600-8-2 pertaining to suspension of favorable personnel actions and AR 380-67 for the suspension of security clearances of persons under investigation.

d. The interim ROI will include a listing of attached exhibits that are provided. These exhibits will be listed as a separate paragraph, but unlike the exhibit section of a final ROI, will not include descriptive summaries. Not attached exhibits may also be listed and are mandatory in accordance with g below.

EXAMPLE

3. The exhibits listed below are attached to supplement this interim report. Upon completion of this investigation and dispatch of a Final ROI, both attached and not attached exhibits will be renumbered to account for additional exhibits collected after the dispatch of this interim report.

a. Attached:

1 - Initial ROI (0001-99-CID000-00001- 5L2B / 5L2C).
2 - Sworn Statement of SSG JONES.
3 - Crime Scene Sketch prepared by SA ADAMS.
4 - Waiver Certificate and Sworn Statement of SPC JEFFERSON.

b. Not Attached:

None

4. Point of contact for this interim is SA John ADAMS, 868-1097.

GUIDO CANDRELLA
Special Agent in Charge

e. The interim ROI may also be used to provide background information in support of a request for assistance (RFA) to another USACIDC unit or other investigative agency. In such instances, it would be attached as an enclosure to the RFA.

f. Use of the interim ROI is optional. Preparation of an interim report would be a waste of time and resources if the proposed recipient only needed copies of statements. The interim report should be used only when less formal means of providing information are not adequate or appropriate.

g. An interim ROI will be prepared when a matter under investigation is to be presented before a federal grand jury. This report is intended to document the results of the investigation up to the point the grand jury begins considering the matter and aid in avoiding the secrecy requirements of Rule 6(e), Federal Rules of Criminal Procedure. This in turn allows the criminal investigation to continue independently of the grand jury investigation and assists in establishing a basis for civil recovery from subjects of the investigation. Interim reports prepared for this purpose will be distributed as follows: one copy each to HQUSACIDC, ATTN: CIOP-COP-CO; USACRC; appropriate group through their subordinate district or field office, and unit file. Copies may be provided to other commanders or agencies as necessary to support administrative action (e.g., suspension or debarment).

7-17
Supplemental ROI

A supplemental ROI advises recipients of additional or corrected information developed subsequent to the submission of a final ROI. (See figures 7-5 and 7-6).

a. The purpose of a supplemental ROI is to re-open an investigation. A Supplemental ROI will be submitted within five business days from the time a need for such action is identified, unless SSI reporting is necessary.

(1) When additional information is developed, but no additional investigative activities have been identified, a Final Supplemental ROI will be sent via ACIRS (with the original mailed to USACRC)**,** without constructing a message formatted "1st Supplemental" ROI. The following are some examples of a Final Supplemental ROI which require no additional investigative activities:

(a) An AFIP consultation report that concurs with the cause and manner of death as previously reported.

(b) A negative toxicology report.

(c) A USACIL report which does not change the outcome of the investigation.

(2) A message formatted "1st Supplemental" will be prepared when additional investigative activities are required. The following are examples of additional investigative activities:

(a) An AFIP consultation report in which the medical examiners have differing opinions on the cause and manner of death as previously reported.

(b) A toxicology report that reflects controlled substance used by the deceased.

(c) A USACIL report which changes the investigative conclusions in the Final ROI.

b. **When** used to report additional investigative activities, supplemental reports will be numbered sequentially, beginning with the “1ST SUPPLEMENTAL.”

EXAMPLE
SUBJECT: CID REPORT - 1ST SUPPLEMENTAL - 0015-99-CID000-00010-5H1B (DIMIS)

EXAMPLE
SUBJECT: CID REPORT - 1ST SUPPLEMENTAL / SSI - 0015-99-CID000-00010-5H1B (DIMIS)

c. The reporting and distribution requirements pertaining to initial, status, and final ROIs, apply to supplemental reports.

d. Subject and victim entry numbers will not be changed after submission of a final ROI. When deletions are made, subject and/or victim numbers will not be reassigned. The ACIRS will automatically enter the words, “Previously Deleted,” when applicable.

EXAMPLE
SUBJECT: CID REPORT - 2ND SUPPLEMENTAL - 0002-99-CID000-00002 - 6E1E1 / 5M2 / 9G1 / 9G2 SUBJECT: 1. PREVIOUSLY DELETED. 2. ARLINGTON, MARY JANE; SGT; 864-00-7463; 20 JUN 78; MIAMI, FL; F; WHITE; A CO, 71ST BN, FORT EXAMPLE, FL 33141; FC; [FALSE SWEARING].

e. When preparing a 1st supplemental ROI, the same format as an initial or status ROI will be used:

(1) Paragraph 6, INVESTIGATIVE SUMMARY. As with initial/status messages, the first paragraph will read as follows, "THE INFORMATION IN THIS

REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY BE CHANGED PRIOR TO THE COMPLETION OF THE INVESTIGATION." The second paragraph will identify the type of report being submitted (e.g., 1ST SUPPLEMENTAL, 2ND SUPPLEMENTAL, etc.) and its intended purpose. A third paragraph will document the facts and circumstances that caused the need for the supplemental. The message will then be completed by repeating of the information reported in the investigative summary of the final report, which will comprise the message's fourth and final paragraphs.

EXAMPLE

6. INVESTIGATIVE SUMMARY: THE INFORMATION IN THIS REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY CHANGE PRIOR TO THE COMPLETION OF THE INVESTIGATION.

1ST SUPPLEMENTAL:

THIS SUPPLEMENTAL REPORT IS BEING SUBMITTED TO ADD MITCHEM AS A SUBJECT OF THIS INVESTIGATION, TO ADD THE U.S. GOVERNMENT AS A VICTIM, AND TO ADD THE OFFENSES OF CONSPIRACY AND FALSE SWEARING.

ON 1100, 23 DEC 98, SGT JONES WAS RE-ADVISED OF HIS RIGHTS, WHICH HE WAIVED, AND REPORTED TO THE FORT BELVOIR CID OFFICE THAT WHEN HE WAS INITIALLY INTERVIEWED ON 24 NOV 98, HE PROVIDED A SWORN STATEMENT HE KNEW WAS FALSE. SGT JONES ADDED THAT WHEN HE STOLE SPC SMITH'S TELEVISION AND VIDEOCASSETTE RECORDER, SPC MITCHEM ASSISTED HIM BY SUGGESTING THAT HE SELL THE PROPERTY AT A PAWNSHOP. SGT JONES ADDED THAT SPC MITCHEM RECEIVED $70.00 FOR HIS ASSISTANCE.

AT 1400, 23 DEC 98, SPC MITCHEM WAS ADVISED OF HIS RIGHTS AND INTERVIEWED. SPC MITCHEM RENDERED A STATEMENT IN WHICH HE ADMITTED TO KNOWING THAT SPC JONES HAD STOLEN SPC SMITH'S PROPERTY, THAT HE SUGGESTED SGT JONES SELL THE PROPERTY AT A PAWNSHOP, AND THAT HE RECEIVED $70.00 FOR HIS INVOLVEMENT.

FINAL REPORT: (REPEAT OF INFORMATION APPEARING ON FINAL REPORT.)

f. In all cases, upon completion of supplemental investigative activity, a final supplemental report will be prepared in the same format as a final ROI, with the following modifications:

(1) Investigative summary. To supplement the previously submitted final ROI, newly developed information will be incorporated into the body of the final ROI and set apart from previously provided information by the use of the phrase "Further investigation…"

EXAMPLE

INVESTIGATIVE SUMMARY:

Investigation established probable cause to believe that SGT JONES committed the offense of larceny when he stole numerous items of SPC SMITH's property, collectively valued at $2,400, and subsequently pawned the items at the ABC Pawnshop, 111 South Central Street, Stafford, VA 22554. SGT JONES, a roommate of SPC SMITH, did not unlawfully enter their room when stealing the items; therefore, the offense of housebreaking is unfounded.

Further investigation established probable cause to believe that SPC MITCHEM committed the offense of Larceny, when he assisted SGT JONES in stealing SPC SMITH's property by suggesting that he sell the property at the ABC Pawnshop. SPC MITCHEM received $70.00 for his assistance. SGT JONES and SPC MITCHEM also committed the offense of Conspiracy, as both acted in concert in the theft of SPC SMITH's property. SGT JONES also committed the offense of False Swearing when, during his initial interview, he rendered a sworn statement he knew to be false.

(2) Status paragraph. This section, as with all final reports, is used to record the status of the investigation, action taken against offenders, or prosecutive status.

EXAMPLE

STATUS: This is a 2nd supplemental report. Commander's report of action (DA Form 4833) is pending.

EXAMPLE

STATUS: This is a 2nd supplemental report. On 8 Dec 98, SGT JONES received a company grade Article 15. SGT JONES was reduced to the rank of SPC, ordered to forfeit $200.00 a month for 2 months, and received 45 days extra duty. Commander's report of action on SPC MITCHEM (DA Form 4833) is pending.

(3) Exhibits/Substantiation. When preparing the exhibit's section of a supplemental report, exhibits will be listed numerically in two separate sections entitled "ADDED ATTACHED" and "ADDED NOT ATTACHED." The numbering process will start based on the last exhibit number reported on the final ROI.

EXAMPLE

ADDED ATTACHED:

16. Agent Investigation Report by SA WOODMAN, 3 Dec 98, detailing the re-interview of SGT JONES, interview of SPC MITCHEM, and additional SJA coordination.

17. Rights Waiver Certificate and Sworn Statement, 23 Dec 98, of SGT Jones admitting to the rendering of a false statement and SPC MITCHEM's involvement in the theft.

18. Rights Waiver Certificate and Sworn Statement of SPC THOMPSON, 23 Dec 98, admitting his involvement in the theft and receiving funds for his assistance.

ADDED NOT ATTACHED:

None

The originals of exhibits 16 through 18 are retained in the files of this office (pending Commander's action).

7-18
Reopened investigations

When a final ROI is returned by HQUSACIDC for additional investigation, the provisions of paragraph 7-17 (Supplemental ROI) will apply.

7-19
Corrected ROI

When administrative corrections are made to a previously submitted final or supplemental ROI prepared in final format, a corrected ROI final will be submitted. The corrected copy ROI will be provided to all previous report recipients, when significant changes were made. In all instances, the original copy of a corrected report will be provided to USACRC.

EXAMPLE

SUBJECT: CID Report of Investigation - Corrected Final - 0015-01-CID000-00010 - 5H1B

7-20
Referred ROI

A referred ROI reports investigative activity conducted or continued by a non-USACIDC agency even though the offense is within USACIDC investigative responsibility. (See chapter 4 for information on the referral of criminal investigations).

a. Initial/SSI/referred, status/SSI/referred and referred ROIs will be prepared in the same format, be given the same distribution, and will be dispatched within the same time restrictions as initial, status, SSI, and final ROIs.

EXAMPLE

SUBJECT: CID REPORT – INITIAL / REFERRED - 0015-99-CID000-00010-5L2B

b. The investigative summary of a referred ROI will reflect the referral.

EXAMPLE

INVESTIGATIVE SUMMARY: THE INFORMATION IN THIS REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY CHANGE PRIOR TO THE COMPLETION OF THE INVESTIGATION.

INVESTIGATION DISCLOSED THAT WHILE SORTING INCOMING MAIL AT THE BATTALION MAIL ROOM, 1/14TH INFANTRY, APO NY 09142, PATTON BARRACKS, MANFRED, GM, SGT JAMES F. FOSTER, 002-95-7635, DETECTED WHAT HE BELIEVED TO BE MARIHUANA IN A LETTER ADDRESSED TO PFC JOSEPH A. NEWMAN, 000-20-0020, CO A, 1/14TH INF, APO NY 09142. NEWMAN STATED THAT SMITH WITHOUT HIS KNOWLEDGE MAILED THE SUSPECTED MARIHUANA TO HIM. ON 22 FEB 93, THIS INCIDENT WAS REFERRED TO THE U.S. POSTAL SERVICE, BALTIMORE, MD., FOR INVESTIGATION.

7-21
Collateral ROI

A collateral ROI is used to report information gathered by a civilian law enforcement agency in which the Army is a party of interest, but for which USACIDC does not have investigative responsibility. This type of report differs from an SSI (ONLY), in that a collateral is assigned an ROI number and usually contains a copy of the civilian law enforcement agency's investigative report as

an attached exhibit. (See paragraph 4-13 for explanation of collateral ROI procedures).

a. The following procedures will be adhered to, when determining the appropriateness of a collateral ROI versus a SSI (ONLY) message report:

(1) When a USACIDC element is made aware of an incident in which the Army is, or may be, a party of interest, but for which the USACIDC has no investigative responsibility for, a sequence number will be initiated.

(2) The interested provost marshal (PM) will be notified and a determination will be made whether the provost marshal will initiate or has initiated a DA Form 3975, Military Police Report, that will be forwarded to USACRC upon completion of the civilian agency's investigation.

(3) If the PM is reporting to USACRC and the information received from civil authorities constitutes an SSI, an "SSI (ONLY)" will be dispatched in accordance with paragraph 7-11. The USACIDC unit may then terminate the action after the SSI (ONLY) is dispatched or, if warranted by the circumstances, continue reporting the progress of the investigation via subsequent SSI (ONLY) reports (e.g., 2D SSI (ONLY), 3D SSI (ONLY), etc.).

EXAMPLE
SUBJECT: CID REPORT - 1ST SSI (ONLY) - 0015-99-CID000-5H1B

(4) If the PM does not intend to report to USACRC and the incident constitutes an offense for which the USACIDC has reporting responsibility, the USACIDC element will prepare a collateral report. Information for the collateral ROI will be obtained from the civilian agency that conducted the investigation. A written police report will be obtained, if it is reasonably available and attached as an exhibit to the collateral ROI. If the police report is not available, the required information may be obtained through interviews of pertinent police personnel.

EXAMPLE
SUBJECT: CID REPORT – INITIAL / SSI / COLLATERAL - 0015-99-CID000-00010-5H1B

(5) When a USACIDC unit submits a final collateral ROI, the ROI will be prepared in the same format as a final ROI. As this type of report merely shadows the conduct of an investigation conducted by a civilian law enforcement agency, there is no requirement to justify early termination in accordance with paragraph 4-17 of this regulation; therefore, collateral ROIs are not closed as Final C reports.

EXAMPLE

STATUS: This is a Final Collateral Report. Commander's Report of Action Taken (DA Form 4833) is pending.

b. See chapter 8 for the distribution of a collateral ROI.

c. Offenses, which are reportable under the VICAP, will, when applicable, be reported with the collateral ROI and in accordance with paragraph 5-38. Care must be taken to avoid duplicate reporting. In cases that are shared with a domestic law enforcement agency, the USACIDC unit should coordinate with the other agency to ensure that duplicate reports are not submitted. If a domestic law enforcement agency is reporting VICAP information, the USACIDC will not report the incident as VICAP and will explain the reason(s) in the investigative summary.

EXAMPLE

INVESTIGATIVE SUMMARY:

This incident is reportable under the Violent Criminal Apprehension Program (VICAP). Coordination with the (appropriate domestic law enforcement agency) has determined that their report is providing the required VICAP information, therefore, this office will not submit duplicate information to the FBI.

7-22
Joint ROI

a. A joint ROI reports the results of an investigation conducted by USACIDC elements jointly with other law enforcement agencies. (See paragraph 4-12 for procedures for conduct of a joint investigation).

b. Joint ROIs will be identified by the word "JOINT" in the subject portion of the ROI. Other law enforcement agencies involved in the investigation will be identified in the Status section of the ROI.

EXAMPLE

SUBJECT: CID REPORT – INITIAL / JOINT - 0015-01-CID000-00010-5H1B

EXAMPLE

SUBJECT: CID REPORT – INITIAL / SSI / JOINT - 0015-01-CID000-00010-5H1B

EXAMPLE

STATUS: This is a final report. This investigation was conducted jointly with the Defense Criminal Investigation Service, ROI number 8800009I-15-APR-01-

c. A copy of the other agency's final report, if available, will be attached as an exhibit. If not available, a description of the investigative effort by the other agency will be included in the appropriate AIR.

7-23
Purpose

a. The AIR is used to document details of investigative findings. The AIR must present sufficient information to describe clearly and concisely the manner in which the subject(s) did/did not violate the law and what evidence was collected in support of the investigative findings. These activities are recorded in chronological order, as they occur, and are not to be used to report recommendations or opinions of the preparer. The primary purpose of the AIR is to:

(1) Records the results of investigative activities while the facts are fresh in the mind of the author.

(2) Provides supportive documentation of the investigative conclusions reached during the course of the criminal investigation.

(3) Serves as a rapid means of providing the results of investigative activities to the action commander, and others having an official need to know, in a timely manner.

(4) Records the results of any type of investigative activity in response to a request for assistance, if a written response is appropriate.

(5) Records information on a preliminary investigation and are later referred to the Military Police for further investigation.

(6) Records those preliminary investigations that are closed without the initiation of an ROI.

7-24
Preparation

a. Fully identify personnel, the first time, by rank, full name, SSAN (if available), and organization or address. Organization designations and addresses will be complete and spelled out to include ZIP codes. Once an organization designation and location have been provided, shortened designations, to include abbreviations, may be used, (e.g., 2/17th FA, 1/2d ACR, etc.).

b. Any number of AIRs may be completed during the course of an investigation. Each AIR should be completed whenever a determination is made that information contained in the AIR is significant information that would assist the action commander or other recipients in completing their responsibilities. The number of AIRs generated during a single investigation is dependent upon many variables, to include the complexity of the investigation and the desire of the CID supervisor. Agent's leaving their offices for a considerable time frame, such as leave, temporary duty, hospitalization, etc., must finalize and sign their AIR(s) before departing.

c. Information in statements or other documents, attached as exhibits, need not be completely restated in the AIR. A summary; however, must be provided to have a chronological flow that "tells the story" of the investigation.

EXAMPLE

At 1400, 31 Oct 98, SPC JONES was advised of his rights by SA HILL. SPC JONES invoked his rights and requested legal representation (See Non-Waiver Certificate of JONES, for details).

d. Pertinent personal observations should be reported in the AIR just as any other relevant information developed during the investigation. In such cases, comments are appropriate if clearly set off from the body of information being addressed. Comments may describe an interviewee's demeanor, the conditions of records, etc. In such instances, the comment will be placed in a separate paragraph, "Agent’s Comment:" immediately following the entry to which it applies. Explanatory sentences may be used to explain actions taken by the agent during the course of the investigation when this information would provide a clear understanding of why such actions were taken.

EXAMPLE

At 1400, 31 Oct 98, SPC JONES was advised of his rights by SA HILL. SPC JONES invoked his rights and requested legal representation (See Non-Waiver Certificate of JONES, for details).

Agent's Comment: During his interview, JONES appeared to be reluctant to answer questions regarding who had borrowed his vehicle on the weekend of 30 - 31 Oct 98 and continuously remarked that he could not recall who used his vehicle during that time frame.

e. The AIR may be prepared and signed by special agents, MP personnel, or other investigative personnel assisting CID investigations (e.g., investigative assistants, investigator/interpreters).

f. Investigative actions, including the time and date of the action, will be recorded on the AIR as soon as possible after completion. Entries will be recorded in complete sentences and written in the third person, past tense. Entries will be typed and single-spaced. Each investigative action will be entered as a separate unnumbered paragraph with double spacing between paragraphs. Since information in the AIR is presented in chronological order, the use of descriptive headings (e.g., Interview of Victim, Interview of Suspect, etc.) are not practical. However, headings such as “Crime Scene Examination, Law Enforcement Records, and Legal Coordination” can be used to draw the reader's attention to important aspects of the report. Continuation pages will be numbered sequentially using additional pieces of bond paper or additional preprinted forms (CID Form 94). The full name and sequence number, if applicable, of each agent and investigator will be recorded the first time he or she is mentioned in the AIR, unless the agent or investigator is the preparer. If the individual is assigned to an office other than the preparing office, the short title of the office will be added, (e.g., Special Agent Sarah P. JONES, 9000, Fort Jackson RA). When the AIR is completed, the words "LAST ENTRY" will be typed immediately after the final entry. Only the first page need be signed by the special agent preparing the AIR. If the special agent is not available to sign the report in a reasonable period, another special agent may sign the report for the preparing agent. Entries in the AIR will be limited to factual, relevant, substantive investigative efforts and findings. (See figures 7-7 , 7-8 and 7-9).

(1) Considerations for documenting investigative activity in AIRs:

(a) Witness interviews, the results of which are not considered significant, will be recorded. Examples might include area canvasses and other interviews which were conducted to cover all possible leads but which result in no pertinent information.

(b) Record the conduct and results of physical and photographic lineups.

(c) Record the results of checks of personnel records, military or civilian.

(d) Record autopsy results and autopsy-related activities, (i.e., exposure of photographs, toxicology results, etc.).

(e) Report the circumstances of obtaining and executing search warrants or authorizations. It may also be used (with modification) for apprehension or arrest warrants.

(f) Record the results of searches and seizure of evidence, other than at the crime scene. Include recoveries of stolen property, obtaining handwriting exemplars and standards, blood and saliva samples, sex crime protocols, etc.

(g) Record computer specific data such as system components, attached peripheral, storage media, software used, etc. (See chapter 12, Computer Related Crimes, for specific documentation requirements).

(h) Record the circumstances of obtaining and serving subpoenas and summonses.

(i) Record the results of credit records checks.

(j) Document personal injuries suffered by any party to the incident under investigation. Entries may consist of personal observations by the investigator, interviews of medical personnel, and results of medical record checks.

(k) Record the results of medical record checks.

(l) Record detailed descriptions and values of property, both stolen and/or recovered. The values of foreign currencies and property will be converted to U.S. currency values using official exchange rates in effect at the time of the incident. This will be accomplished by citing the exchange rate used and listing, in parenthesis, the U.S. currency value immediately following the foreign currency value.

EXAMPLE
Agent's Comment: According to SPC SMITH, he was robbed of currency and property valued at $135.00 and German marks (DM) 1,150.00 ($363.92). The exchange rate used was $1.10 to 3.16 DM.

The value of stolen U.S. Government property will be obtained from the official catalogs or pricing lists in effect at the time the property was stolen, if the property was in a serviceable condition. If the stolen property was obsolete or unserviceable, a lesser-estimated value will be shown, as established by a person who, by training or profession, is in a position to know or compute the value. The value of stolen private property will be its legitimate market value at the time it was stolen. This will be determined by the value of like items presently being sold on the open market, from the owner of the property, or from an individual who, by training or profession, is in a position to know the value (See Article 121, Manual for Courts-Martial, for further guidance on property value estimates). All recovered property and its value will be accounted for and reflected in the AIR, regardless of the agency responsible for the recovery. The value of recovered non-appropriated property will be the same as the value reported lost or stolen, regardless of condition. When property is recovered in a damaged condition, the extent of these damages will be reflected. When available at the time the final report is written the actual cost of repairs will be shown as the amount of damage. If not, an estimated amount of damage will be obtained from the owner, an insurance company, or repairman. If component

parts are missing from the recovered property, their present market value will be subtracted from the recovered value.

(m) Record the disposition of subjects who were apprehended during the investigation.

(n) Record the results of coordination with other law enforcement agencies.

(o) Record results of coordination with other agencies or officials, where such coordination is relevant to the investigation. Entries, which address routine coordination with commanders, need not be reflected in an AIR. Such administrative entries are best documented in the case's Agent's Activity Summary (AAS).

(p) Record the results of surveillance activities.

(q) Record the results of consensual intercept operations. A distinction between consensual and nonconsensual intercept should also be made.

(r) Record the results of interviews of sources whose identities are protected. Confidential or registered sources will not be identified on the AIR. Sources will be referred to as "source" or "CID source". Source identification numbers will not be recorded in the AIR.

(s) Record the local analysis of the information provided prior to initiation of covert operations.

(t) Record source searches before and after controlled purchase operations.

(u) Record pertinent information on the issuance of official agency funds for controlled purchases or other activities.

(v) Record the circumstances of controlled purchases, including amount spent, items purchased, and other pertinent details.

(w) Record the conduct of drug field tests. When field test results are reported, a copy of CID Form 36 (Field Test Analysis of Suspected Controlled Substances) will be attached to the ROI as an exhibit.

(x) Record a concise summary of significant laboratory examination results in a manner understandable to a non-police layperson. This may include information that is not readily apparent from a reading of the laboratory examination report such as the interrelationships of important evidence.

EXAMPLE

On 1 Mar 99, USACIL laboratory examination report #99-CID131-0001 was

received and reflected that a fingerprint lifted from the revolver found at the crime scene was made by SGT BRICHACEK. The report also noted that the bullet recovered from the body of the victim had been fired from the same revolver.

(y) Record objective personal observations by investigators that are not reported elsewhere. These observations or comments should be set aside from AIR entries with the words, “Agent’s Comment:” prior to the first sentence.

(z) Investigative support and "housekeeping" activities will not be recorded in the AIR except in very unusual circumstances. In addition to examples discussed elsewhere in this regulation, unnecessary entries include briefings of USACIDC personnel, guidance from USACIDC personnel, dispatches of requests of assistance, turn in of evidence, etc.

(aa) Document special program information in cases, such as fraud, economic crime, and public corruption category investigations to describe briefly a specific or little known DoD program, procedure, or regulation crucial to understanding the offenses and thrust of the investigation.

(bb) Law Enforcement Records. Record the releasable results of file checks of the DCII and, if appropriate, other federal, state or local law enforcement records. Preparation of the final report will not be delayed pending results of record checks.

(cc) Crime Scene Examinations. This paragraph provides the name of the examiner and the time, date and location of the examination and may include any of the following sub-paragraphs:

1. Characteristics of Scene. Provides a description of the general features of the crime scene area. It would normally include a description, as applicable, of the building, room, furniture, doors, windows, relationship of the scene to other facilities, buildings, or activities in the area, occupation by personnel, etc. This paragraph provides the reader with a general understanding of the area.

2. Condition of Scene. Describes those aspects that are variable based on particular circumstances. The state of cleanliness, disarray, whether objects are wet, dirty or contaminated with other substances, evidence of ransacking or forced entry, etc., would be discussed. The presence of odors or other similar observations would also be mentioned in this section.

3. Environmental Conditions. When appropriate, this paragraph may be used to report on the weather conditions or other environmental factors of significance to the investigation. Observations that are considered significant could be temperatures, precipitation, snow accumulation, etc.

4. Factors Pertinent to Entry/Exit. Describes the probable routes of entry to or exit from the scene, including any other specific information of interest. Normally an entry in this paragraph is appropriate even if it is similar to: "Being an open area, access could be gained from any direction." It is important, however, to report only objective observations. Speculation, such as "apparently entrance was gained through the office's window", should be avoided, unless supported by specific facts that eliminate other possibilities (e.g., broken window, footprints or window ledge, etc.).

5. Scene Documentation. Describes how conditions at the crime scene were documented. Usually this will consist of preparation of a crime scene sketch and the taking of photography. When no photographs are exposed, an entry explaining the lack of crime scene photographs will be made.

6. Search for Latent Impressions. The results of fingerprint processing are reported in this paragraph. When large amounts of fingerprint evidence are collected, a log of the specific location of each lift may be attached as a separate exhibit and referenced in this paragraph.

7. Collection of Crime Scene Evidence. Records the collection of physical evidence at the crime scene, or a negative entry that no evidence was discovered during processing.

7-25
Request for assistance (RFA)

a. General:

(1) A RFA is a request forwarded outside of the originating USACIDC unit's area of responsibility to collect information or evidence necessary to complete the investigation. When appropriate, the RFA should be directed to either another USACIDC unit or to a non-USACIDC agency. If there is no specific requirement for special agent involvement in obtaining the required information, then alternate methods for obtaining the information should be considered and used. Direct correspondence with governmental offices/agencies or with business offices is encouraged as a means of conserving investigative resources and expediting completion of such requests. Special agents and supervisors are responsible for insuring that only RFAs for obtaining meaningful investigative information are dispatched. Telephonic interviews in lieu of RFAs are encouraged where appropriate. In many instances, it is a waste of USACIDC resources to routinely require face to face meetings with witnesses who are not locally available when the required information can be easily obtained by telephone and documented in the AIR.

(2) There is no prescribed format for a RFA. It may be prepared in any convenient format and transmitted verbally, in writing, or by other means to include facsimile machine or electronic mail. In any case wherein sensitive or potentially embarrassing information is being transmitted, prior coordination will be made with the receiving element to advise them that the information is being transmitted, and to verify that the mode of transmission will ensure the information is not released outside of CID channels. The receipt of a RFA will be confirmed in some manner such as by transmitting a reply via electronic mail. At a minimum, the RFA must contain:

(a) Requesting unit's sequence/ROI number.

(b) A clear statement of the assistance requested.

(c) Sufficient information to allow the receiving agency or USACIDC unit to respond adequately without need of further amplification. Copies of supporting documents or exhibits will be provided with the RFA, as necessary.

(d) Any known data about individuals to be interviewed that requires special handling, care, or caution when approaching or confronting the individual(s). This would include the following:

1. The individual is known to be armed, to include the types of weapons carried or used.

2. The individual is known to have a violent temper, is prone to violence, or is known to assault law enforcement officers.

3. The individual poses a potential health hazard because the individual has been diagnosed as having known transmittable diseases. Disseminating information on AIDS victims/carriers requires careful consideration and handling because significant individual privacy rights are at stake. Providing information about an individual with AIDS or similar health risks will only be done when there is reason to believe there is significant danger to agent(s) who will have contact with the individual or if the information is of significance to the offense(s) under investigation.

4. The individual has a health problem that should be known and considered for the individual's own protection, i.e., severe heart condition, subject to epileptic seizures, or any other condition that could be triggered by the stress of a confrontation with law enforcement personnel.

5. Any other information that would assist the responding unit in dealing with the individual, such as, known to flee if not closely guarded, has escaped previously by climbing out of windows, hides drug stash in certain places, etc.

(3) A RFA may be made telephonically without written follow-up only when minimal investigative effort is required of the receiving unit.

(4) A RFA will be forwarded directly to the unit in whose area the lead is to be worked. Information copies are not required for higher HQs.

(5) A RFA requiring investigative activity in a country in which no USACIDC units are located will be forwarded to the headquarters of the USACIDC major subordinate command responsible for the area. Areas of responsibility for each USACIDC major subordinate command are described in CIDR 10-1.

(6) When assistance is required from the headquarters of a federal investigative agency, the RFA will be forwarded to the Federal Liaison Officer, HQUSACIDC, ATTN: CICG-FLO, for action.

(7) A copy of a written RFA and of the written reply (information report) will be included in the case folder of the requesting USACIDC unit. Verbal requests and replies will be noted in the AAS and as appropriate, an AIR.

(8) The need for written RFAs will be determined on a case by case basis. Unit policies, which strictly require or prohibit written RFAs are prohibited.

b. Special procedures

(1) U.S. Postal Service (USPS) money orders. The following procedures will be used when requesting original USPS money orders and other original USPS documents:

(a) A USACIDC unit having a requirement to obtain USPS money orders and other documents as evidence will submit their requests to the St. Louis Branch Office (BO), USACIDC. The St. Louis BO will obtain the requested items and forward them as evidence to the requesting office.

(b) The RFA will include the serial number, date, dollar amount of the money order, post office of issue, purchaser, and name of payee, for each money order requested.

(c) When original money orders and other postal documents are no longer needed for evidence purposes, they will be returned by evidence disposal procedures to the St. Louis BO, for return to the USPS.

(2) An RFA to obtain financial documents from the Defense Finance and Accounting Service, Indianapolis-Center, Indianapolis, IN, must be made in writing to the Indianapolis Fraud Resident Agency (RA), USACIDC. A RFA may be transmitted via mail channels, facsimile, or electronic mail.

(a) To request BAS, and BAH related documents, requests must contain, as a minimum, the following information:

1. Name (of the individual to whom the documents pertain).

2. SSAN (of the individual identified above).

3. Date (YYMM) (date of the requested records).

4. Update number (2 digits).

5. Army disbursing station number (ADSN) (4 digits).

6. Cycle number (2 digits - 1 alpha, 1 numeric).

7. Transaction number (4 digits).

(b) To request travel related documents, the following information, as a minimum, is required:

1. Name (of the individual to whom the documents pertain).

2. SSAN (of the individual identified above).

3. Date (YYMM) (date of the requested records).

4. Voucher number (of the requested document).

5. ADSN.

The information required in subparagraphs a(2)(a)4 and a(2)(a)7 above are reflected on the service member's Master Military Pay Account (MMPA) and the Daily Transmittal Record (DTR), and must be obtained from the supported Defense Military Pay Office (DMPO). The information required in a(2)(b)4 and a(2)(b)5 are available from the service member's Integrated Automated (Army) Travel System (IATS), and also must be obtained from the supported DMPO.

(3) U.S. Savings Bonds:

(a) Worldwide requests for original or copies of savings bonds will be forwarded to the servicing USSS office, after verification that the owner has submitted a claim to the appropriate DMPO or other agency.

(b) The RFA should provide the requesting element's control number and the following data concerning the savings bond:

1. Complete serial number to include letter.

2. Complete name(s) of the registered owner(s).

3. Denomination.

4. Address(es) on the savings bond.

(4) U.S. Treasury Department (USTD) checks:

(a) Paragraph 4-9c contains special instruction for investigations involving USTD checks.

(b) Requests for original or copies of USDT checks will be submitted through the servicing USSS office. These RFAs should provide the requesting unit's sequence/ROI number and as much of the following data as can be obtained.

1. When the check was negotiated, a copy of the check should be attached, if available.

2. Whether the payee initiated a stop-payment request and if so, when. A copy of the stop-payment request should be attached, if available.

3. If not otherwise provided: The check number; symbol number; date of check; amount of check; name of payee as reflected on the check; disbursing office.

(c) When checks received from the servicing USSS office are no longer needed, they will be returned to the servicing USSS office by registered mail.

(d) When USTD checks are seized as evidence prior to being processed by the U.S. Treasury, they will be returned when no longer needed to the DMPO that issued the check (identified by the DSSN on the face of the check). Checks issued by other departments of the federal government will be returned to the issuing agency at the address printed on the face of the check. All checks will be returned by evidence disposal procedure. A letter of transmittal will accompany all returned checks.

(5) PM Support:

(a) In order to comply with the USPS and USTD desires for a single point of contact within each department, all USACIDC units located overseas will process document requests for local PM activities.

(b) Upon receipt of a RFA, a sequence number should be initiated for the action and a RFA forwarded to the servicing USSS office using the procedures

outlined in the preceding paragraphs. Additionally, a DA Form 209, Delay Referral or Follow-up Notice, will be attached to the RFA. Upon receipt of the DA Form 209 from the servicing USSS office, the file should be suspended for 120 days from the date of the DA Form 209. A status letter should be forwarded to the servicing USSS office at that time and every 90 days thereafter until the documents/money orders are obtained. Upon receipt of the requested documents/money orders, they will be released to the requesting PM and the sequence number will be closed.

(c) If the documents/money order can be released to the PM on the same day they are received from the servicing USSS office, it is not necessary for the evidence to be processed through the CID evidence room. When the document(s) have been released to the PM.

c. Follow-up action. If response to a RFA is not received within a reasonable time, the requesting USACIDC unit will inquire as to the status. A DA Form 209 will accompany RFAs submitted to St. Louis BO for postal money orders or USSS for savings bonds and treasury checks. Inquiries as to the status of these RFAs should be made approximately 120 days after the RFA was forwarded. Inquiry should be made relative to other RFAs in approximately 30 days.

d. Request for assistance concerning transient personnel. A RFA requiring the interview of an individual who has transferred overseas area will be handled as follows:

(1) When the individual's new permanent assignment is known, a RFA should be forwarded to the appropriate USACIDC unit. A copy of the pertinent movement order should be included.

(2) In the instance where the individual has been assigned to an overseas replacement unit for further assignment, the requesting unit should query the appropriate USACIDC major subordinate command to determine the permanent assignment of the individual. This query will contain the following: Sequence/ROI number; full name; rank and SSAN; MOS; DOB; former unit of assignment; orders number, date of movement orders; reporting date; and number of days leave to be taken prior to arriving at the replacement unit. Within five business days of receipt, the USACIDC major subordinate command will determine and verify the permanent assignment and will respond to the requesting USACIDC unit advising them of the confirmed assignment and the responsible USACIDC unit. The requesting office should send the RFA directly to the USACIDC unit cited in the USACIDC major subordinate command message. In the event the individual has not yet reported to the overseas replacement unit, the USACIDC major subordinate command will advise the requesting unit and suspense rechecks for every ten working days or less, depending upon the seriousness of the RFA.

e. Interagency investigative support between Defense Criminal Investigation Organizations (DCIO):

(1) All USACIDC units will make every effort to provide support to a requesting DCIO.

(2) In the event an office is unable to comply with the lead request due to a lack of appropriate expertise or other operational difficulty, the receiving office will provide such support to the requesting agency as it is able. Support might include suggesting other avenues for completion of the request, and coordination with local authorities to provide office space and transportation to arriving agents.

(3) A USACIDC unit should submit a RFA to a DCIO when the request significantly enhances timeliness, efficiency and/or economy of operation. Send requests to DCIOs that are located as near as possible to the area where assistance is needed. Prior coordination will ensure that the recipient office has agents trained in the appropriate investigative disciplines to effectively respond to your request and the lead location falls within the recipient's area of responsibility.

(4) The timeliness guideline for handling a DCIO RFA is within 20 calendar days. Extensions of this time period must be negotiated with the requesting DCIO. A DCIO unit may request more expeditious handling of particularly urgent requests.

(5) If there is no specific requirement for special agent involvement in obtaining the required information, then alternative methods for obtaining the information should be used. Direct correspondence with government offices/agencies or with business offices is encouraged as a means of conserving investigative resources and expediting completion of requests.

(6) To track the number of RFAs submitted to DCIOs, the following data must be entered in ACIRS:

(a) Ensure the "Action Type" data field is reported as "RFA" under General Case Data.

(b) In the same data area, the "Inves. Agcy" data field must be completed with the DCIO agency requesting support and the "RFA Case No." data field must be completed with the requesting DCIO's case number.

(7) The USACIDC unit receiving the RFA must provide the following data in the information report for the requesting DCIO.

Agent Hours: 16
Administrative Hours: 2

Travel Hours: 6
Travel Costs: None
Per Diem Costs: None
Investigative Costs: $10
Court document fee: $15
Source payment: $100
Other Costs: $200
Rental of storage locker: $50
Document reproduction: $30 (film)

(8) During the course of an investigation, all RFAs to DCIOs must be tracked on a sequence number in the same manner as requests to USACIDC units with the addition of the cost savings. Record the total cost savings for each request to a DCIO at the bottom of the CID Form 66. The cost savings are a best guess estimate based on personnel costs, travel, lodging, equipment usage and other costs.

7-26
Information report

a. When a USACIDC unit receives a RFA, it will initiate a sequence number, promptly acquire the information requested, and provide a response by an information report within 15 business days. However, no sequence number is required when a telephonic answer will suffice. When an information report cannot be dispatched within 15 business days, the requesting office will be notified of the reason for non-completion by the most expeditious means possible.

b. There is no prescribed format for information reports. They will be provided to the requesting unit, verbally or in writing, by the most appropriate means. Information reports will contain all requested information. The responding unit will provide the total investigative, travel and administrative time expended to the requesting unit. If a message response is provided, no further written response is required.

c. Information reports are forwarded directly to the requesting unit. Information copies to other USACIDC units are not required.

d. A copy of a written request for assistance and of the information report will be included in the case folder of the USACIDC unit providing the assistance.

7-27
Agent's Activity Summary (AAS), CID Form 28

a. An AAS will commence whenever a sequence number is initiated and used to record information relevant to that sequence number. (See figure 7-10).

b. The AAS should allow for the reconstruction of the manner in which an investigation was conducted, in the event responsibility is transferred to another special agent or USACIDC unit.

c. To avoid duplication, the AAS will, when possible, be used to summarize investigative activities and refer to the source documents or AIR contained in the case file. If the AAS does not reference information documented in other documents, all entries in the AAS must be in sufficient detail to provide a complete understanding of the activity.

EXAMPLE

AGENT'S ACTIVITY SUMMARY	
TIME, DATE, AND AGENT	SUMMARY OF INVESTIGATIVE ACTIVITY
1200, 31 Oct 98 SA FURR, (1:40 INV)	Conducted crime scene examination (See AIR and sketch for details).
1205, 31 Oct 98 SA WOODMAN (:15 TRVL)	Transported victim to CID office.
1220, 31 Oct 98 SA CONSTABLE (1:30 INV)	Interviewed SPC SMITH (See statement for details).
1300, 3 Nov 98 SA MONTANO (1:30 INV)	Interviewed SGT WALTERS (See statement for details).

d. The AAS, or copies thereof, will not be released outside USACIDC channels except as authorized by Chapter 25 or in response to a court order or a ruling by a military judge. However, the AAS may be subject to inspection by defense counsel pursuant to a proper discovery request to a trial counsel under Rule 701, Manual for Courts-Martial.

(1) Trial counsels and defense attorneys must be allowed to inspect the AAS after a subject of the investigation has been served charges in accordance with R.C.M. 602, Manual for Courts-Martial.

(2) All other requests from outside USACIDC to inspect the AAS will be referred to the Director, U.S. Army Crime Records Center in accordance with Chapter 25 of this regulation.

(3) As stated in MCM, Rule 701(h), “inspect” includes the right to read, photograph and copy a document.

e. The AAS will be used solely for those activities germane to the particular sequence number. In addition to recording relevant investigative, administrative, and supervisory activities, the AAS, as an inner office form of communication, may be used to record subjective opinions and impressions made by USACIDC personnel regarding a particular case. The AAS, however, will not be used as a means of documenting personal grievances, performance evaluations, administrative or disciplinary sanctions against USACIDC personnel, or for any similar purpose.

f. The AAS will be used to aid accountability and entry of direct workload (work-hour) data in ACIRS.

7-28
Interview worksheet (CID Form 44)

a. The CID Form 44 is used to record personal information on suspects, subjects, victims and witnesses interviewed in connection with investigations. The form, when used, will be retained in the case folder. The extent to which the form is completed is optional and dependent upon the needs of the investigating agent.

b. Preparation of the CID Form 44 is discussed in detail in the ACIRS User's Manual.

7-29
Crime Records Data Reference Card (DA Form 2804)

a. The DA Form 2804 is a manual system to use when the ACIRS is not available.

b. A separate DA Form 2804 will be prepared and attached to the front of final, referred, collateral, and supplemental (when used to report new investigative information) ROI for each of the following:

(1) Each individual, firm, or other legal entity listed in the subject section of the ROI. If the individual is being deleted from the subject section, the word "Deletion" will be entered in the remarks section of the form.

(2) Each individual, U.S. Government agency or organization, private firm or corporation, or other legal entity listed as a victim in any ROI. If the individual is being deleted from the victim section, the word "Deletion" will be entered in the remarks section of the form.

(3) Each alias or other name, to include the maiden name and any present or former names, of individuals for whom a DA Form 2804 has been prepared in accordance with paragraphs (1) and (2) above when different personal identifiers (DOB or SSAN) are used. All known names, and all appropriate personal identifiers will be listed in item 6, or if insufficient space is available, in the remarks section or on the reverse side of the form.

(4) When there is no change in personal identifiers each alias or other name, to include the maiden name and any present or former name, will be entered in block 6, or if insufficient space is available, in the remarks section or on the reverse side of the form. There is no requirement to prepare separate forms for each name in this situation.

(5) When the listed subject or victim is in a fugitive deserter status, the words "Fugitive Deserter" will be entered in the remarks section of the form.

(6) When executing DA Form 2804 for a corporation, the address of the corporation will not be included. This is to ensure that a corporation name check will be completed. A corporation having several locations will have an incomplete name check if an address is included in the magnetic media.

c. The first copy of the card will be forwarded with the final or supplemental ROI to USACRC. The second copy may be retained and placed in the unit name index file.

d. Preparation of DA Form 2804 on persons connected with ongoing investigations for use in the unit name index file is authorized at the discretion of the CID supervisor. Such cards must be clearly identified as "Investigation Pending" cards.

7-30
Criminal Intelligence Report (CID Form 97)

a. During the conduct of an investigation, criminal intelligence related to the investigation of interest only to special agents and their supervisors may be developed. The CID Form 97 will be used to record this information and

processed as required under chapter 18 of this regulation. Information pertaining to investigative delays, lack of photography, polygraph declinations, and other internal administration information should be documented and forwarded within USACIDC channels via a memorandum for record. As this information is not related to criminal intelligence, the use of a memorandum is considered appropriate for this purpose. (See figure 7-11).

b. Information on modus operandi, new methods or techniques for the commission of crimes, and developed information which is not a part of a ROI should be extracted and reported separately in accordance with chapter 18.

7-31
Document Cover Sheet (CID Form 14)

a. A Form 14 will be affixed on top of the first page of any CID originated investigation-related document or series of documents transmitted outside USACIDC channels.
(See figure 7-12).

b. When the ROI contains classified defense information, the words "FOR OFFICIAL USE ONLY" will be lined out, and the document cover sheet will be stamped "CONFIDENTIAL", "SECRET" or "TOP SECRET" as appropriate. In addition, compliance is required with the provisions or AR 380-5, regarding DA Labels 22, 23, and 24 (classified document cover sheets) which will be placed on top of the CID Form 14.

7-32
Commander’s Report of Disciplinary or Administrative Action Taken (DA Form 4833)

a. For each person listed as a subject of a founded criminal offense in a final, collateral or supplemental ROI, a DA Form 4833 (See figure 7-13) will be submitted, unless the action can be reported in the "Status" section of the ROI. Action taken against subjects will not be reflected in the investigative summary of the ROI. A DA Form 4833 will not be submitted for person(s) listed in unfounded or insufficient evidence ROIs (see paragraphs 7-6c(2) and 7-6c(3).

b. An Action Commander's Memorandum of Transmittal (MOT) (See figure 7-14) will be forwarded with the ROI to the action commander, through the next higher field grade commander, for each subject listed in a founded ROI. The action commander for all cases wherein Defense Intelligence Agency (DIA) personnel are listed as subjects is Headquarters, DIA. (See subparagraph 7-32m). The DA Form 4833 will be completed down to the "Action Taken" section

by the reporting USACIDC unit prior to dispatch to the action commander. In the event the action commander takes action against the soldier for an offense other than the one(s) listed in the CID report, the revised offense will be specified in the REMARKS section (block 15) of the DA Form 4833. The DA Form 4833 will be attached to the front of the final report underneath the MOT. The action commander is required to complete and return the DA Form 4833 through the next higher field grade commander in accordance with AR 195-2 and AR 190-45, Law Enforcement Reporting, 20 October 2000. The DA Form 4833 will have a 45-day suspense IAW AR 190-45. (There is currently a conflict between AR 195-2 and AR 190-45 concerning the suspense date. This conflict will be resolved with the new publication of AR 195-2.)

c. If the action commander fails to complete and return the DA Form 4833 within 45 days, another MOT annotated "second request" along with a new DA Form 4833 will be forwarded with a 15 day suspense. If there is no response to the second request, direct coordination with the addressees or appropriate staff members should be accomplished in order to have them complete the DA Form 4833. (ALCID 002-03)

d. Prior to forwarding the DA Form 4833 to USACRC, the USACIDC unit will review the action commander's entry to insure that all required data is included.

e. Reports from action commanders that action is still pending will not be forwarded to USACR C. Suspense dates will be adjusted on a case-by-case basis.

f. When information on action taken is obtained verbally, the DA Form 4833 will be addressed to USACRC from the reporting USACIDC element. The person developing the information will sign the form and the title “commanding officer” in the signature block will be lined out. In the event the action commander takes action against the soldier for an offense other than the one(s) listed in the CID report, the revised offense will be specified in the REMARKS section (block 15) of the DA Form 4833. (ALCID 002-03)

g. The completed DA Form 4833 will be forwarded to USACRC. When originals of exhibits not previously attached to a ROI are forwarded to USACRC, they will be recorded in the remarks section of the DA Form 4833.

h. A copy of each DA Form 4833 forwarded to USACRC will be included in the case folder at the preparing USACIDC unit.

i. A copy of each DA Form 4833 forwarded to USACRC will be provided to the SJA having jurisdiction over the subject(s). A copy will also be provided to the PM responsible for the area in which the incident occurred.

j. Action taken against non-DoD civilians will be developed through coordination with the SJA, local courts, or police agencies. This may require action described in paragraph 4-29 (suspension and debarment activities). The DA Form 4833 will be addressed to USACRC from the reporting USACIDC unit and completed as per the instructions in paragraph (f) above.

k. When a major overseas commander cannot be identified as the action commander for subjects not subject to the UCMJ, a copy of the ROI should be forwarded to HQUSACIDC, ATTN: CIJA-ZA, which will process the action and provide the necessary data for completion of the DA Form 4833 to the originating USACIDC unit. (See paragraph 8-16).

l. Upon receipt of action taken, the investigating field element will update the ACIRS database with the action taken information.

m. The DA Form 4833 for cases wherein DIA personnel are listed as subjects will be forwarded to the Defense Intelligence Agency (ATTN: DIAC, Freeman, IG), Bldg 6000, Washington, DC 20340-5100, for completion.

7-33
Workload (work-hour) reporting

a. All USACIDC field elements will utilize the ACIRS to record workload data associated with all sequence numbers and ROI actions. The ACIRS system classifies time expended on workload into seven work-hour categories: investigative hours, investigative administrative hours, administrative hours, travel hours, supervisory and other agent hours, post final report hours, and polygraph hours. The activities, which comprise these seven categories, are defined below.

(1) Investigative hours. Time expended by investigative personnel in the conduct of investigations or investigative related activities. Investigative personnel are special agents, MP and non-MP personnel assigned/attached to USACIDC unit, civilian criminal intelligence coordinators, and investigative operations assistants, who have been issued USACIDC credentials by the respective USACIDC unit commander. These hours include hours expended by USACIDC supervisors who are dual hatted and also perform pure investigative duties. This category includes time expended by evidence custodians in the collection of evidence at crime scenes. This category also includes local travel hours expended by investigative personnel traveling to and from a particular location (e.g., crime scene) to conduct a preliminary investigation, collect evidence, conduct interviews, coordinate with appropriate activities/agencies and other official activities normally associated with criminal investigations or investigative actions. All work hours expended by special agents, MPI, DST personnel, etc., monitoring a polygraph examination, and all work-hours

expended by female witnesses observing the testing of female examinees will be reported as investigative hours. All time expended by investigative personnel preparing statements, evidence vouchers, subpoenas, warrants and similar documents will be classified as investigative hours and captured under this field.

(2) Investigative administrative hours. Time expended by investigative personnel in administrative functions directly related to specific investigations or investigative actions. Investigative administrative functions include filing, copying, preparing name check files, preparing source reports, administering the .0015 fund program, preparing case folders, preparing draft final reports, making ACIRS' entries, collating ROIs and associated documents for filing and distribution, and final disposition of reports and case files will be classified as investigative administrative hours and captured under this field.

(3) Administrative hours. Time expended by non-investigative personnel performing those same functions described in the investigative administrative work-hour category.

(4) Travel hours. Time expended by investigative personnel in a travel status, to and from a destination beyond the normal duty station and adjoining communities, when conducting any investigative related activity. This category includes time expended in pre-travel and post travel activities such as making travel arrangements/flight reservations and preparing travel vouchers. This category does not include time at the final destination, which is chargeable under the "investigative hours" category.

(5) Supervisory and other agent hours. Time expended by USACIDC supervisors providing direct management and oversight of any investigative related activity for investigative and administrative sufficiency. This category also includes time expended by evidence custodians in the receipt, management, and disposition of evidence, including all related travel time.

(6) Post final report hours. Time expended, including all related travel time, on investigations after completion of the "final" ROI and on other investigative related actions after those actions are "closed" in ACIRS. This time includes court appearances, attendance at administrative hearings, courts-martial, all time expended by personnel preparing for, traveling to and from, and testifying in court or other hearings, and processing of DA Forms 4833. Work-hours expended on ROIs re-opened for further investigation by a supplemental ROI will be reported in ACIRS as investigative, investigative administrative, administrative, travel, supervisory, or polygraph, as appropriate. These work-hours should be added to those previously reported to reflect a total accumulated work-hour figure.

(7) Polygraph hours. All work-hours expended by USACIDC polygraph examiners providing polygraph support to field elements. Work-hours expended

by polygraph examiners include the review of open cases for potential polygraph utilization, the review of case materials prior to testing, actual polygraph testing, preparation of polygraph test results, and interviews and interrogations performed by examiners in non-polygraph settings. These work-hours also include all travel time expended by polygraph examiners in accordance with paragraph 7-32a(4) above. It is not necessary that a polygraph examination be conducted to report work-hours expended by a polygraph examiner. (For example, a rape subject consents to a polygraph examination and appears at the USACIDC office on the date of the scheduled examination. However, during the pre-test phase of the examination, the subject elects not to take the polygraph. The work-hours expended by the examiner in reviewing the case materials would be reported as polygraph work-hours. All travel hours expended by the examiner, if appropriate, would be reported as travel hours). Work-hour information will be provided the polygraph examiner to the investigative case agent or special agent-in-charge at the time polygraph provides support. In those instances wherein polygraph support is provided to local commanders, trial defense service offices, and provost marshals, a CID action record will be initiated so as to reflect total polygraph work-hours expended, in addition to any other category of work-hours listed in subparagraphs a(1) through a(6) above.

b. All USACIDC units will report workload data in ACIRS for protective service sequence actions in accordance with paragraph 6-2c(6) of this regulation only for work-hours expended by CID special agents assigned, attached or in temporary duty status to the field element which initiated the sequence action. Field elements will not report protective service work-hours expended by special agents assigned to the Protective Services Unit (PSU), USACIDC, or work-hours expended by agents of any other federal agency or DoD component engaged in protective service activities. The reporting of protective service work-hour data by field elements pertains only to those short-term protective service missions normally conducted within a field element's geographical area of responsibility, and does not include those instances in which special agents are detailed to the Protective Service Unit for long term commitments.

c. Work-hours expended by USACIL examiners pursuant to laboratory examinations of evidence submitted by USACIDC field elements will not be reported as workload data in ACIRS.

d. All USACIDC supervisors designated as an approving authority for the release of USACIDC reports will ensure workload data is correctly documented in all completed sequence numbers prior to the transmission of such reports to the USACRC by ACIRS.

Figures

7-1 Initial Report Format

7-2	Status Report Format
7-3	Final Report Format
7-4	Interim Report Memorandum
7-5	1st Supplemental Report Format
7-6	2nd Supplemental Report Format
7-7	Agent's Investigative Report (Non-Form)
7-8	Agent's Investigative Report (Form)
7-9	Agent's Investigative Report (Form)
7-10	Agent's Activity Summary
7-11	Internal USACIDC Memorandum for Record
7-12	CID Form 14, Document Cover Sheet
7-13	DA Form 4833, Commander's Report of Disciplinary or Administrative Action
7-14	Action Commander's Memorandum of Transmittal (MOT)
7-15	Initial/Final ROI

Figure 7-1. Initial Report Format

DATE: 10 JAN 99 17:30
FROM: SAC USACIDC RES AGCY FORT EXAMPLE FL //CIRCW-FEF//
TO: DIR USACRC USACIDC FORT BELVOIR VA //CICR-ZA//
PROVOST MARSHAL FORT EXAMPLE FL 33141
SJA FORT EXAMPLE FL 33141
CDR A COMPANY, 71ST ORD BN FORT EXAMPLE FL 33141
CDR USACIDC 2D MP BN FT STANDARD GA 22102 //CIRCW-FSG//
CDR 3RD MP GROUP (CID) FORT GILLEM GA //CIRC-ZA//
CDR USACIDC FT BELVOIR VA //CIOP-ZA//

SUBJECT: CID REPORT OF INVESTIGATION - INITIAL/SSI – 0002-99-CID000-00002 – 6E1E1

DRAFTER: HUDSON, KATHI L.
RELEASER: CANDRELLA, GUIDO

UNCLASSFIED - FOR OFFICIAL USE ONLY

1. DATES/TIMES/LOCATIONS OF OCCURRENCES:
1. 10 JAN 1999/0630 - 10 JAN 1999/0700; SUNSET ROAD, ADJACENT RANGE NUMBER 3, FORT EXAMPLE, FL 33141

2. DATE/TIME REPORTED: 10 JAN 1999, 0800

3. INVESTIGATED BY: SA TAZ MONTANO, 4039; SA KATHI L. HUDSON, 4812; SA ROLLING E. HILL, 4366

4. SUBJECT: 1. JOHNSON, MATHEW WILLIAMS; SGT; 635-85-7456; 7 AUG 1979; COLUMBIA, SC; M; OTHER; A COMPANY, 71ST ORDNANCE BATTALION (A CO, 71ST ORD BN), FORT EXAMPLE, FL, 33141; TC; [RAPE].

5. VICTIM: 1. ARLINGTON, MARY JANE; SGT; 864-00-7463; 20 JUN 78; MIAMI, FL; F; WHITE; A CO, 71ST ORD BN, FORT EXAMPLE, FL 33141; TC; [RAPE].

6. INVESTIGATIVE SUMMARY: THE INFORMATION IN THIS REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY CHANGE PRIOR TO THE COMPLETION OF THE INVESTIGATION.

THIS INVESTIGATION WAS INITIATED UPON NOTIFICATION BY THE FORT EXAMPLE MILITARY POLICE THAT SGT ARLINGTON REPORTED SGT JOHNSON HAD RAPED HER.

ON 10 JAN 99, SGT ARLINGTON REPORTED THAT WHILE JOGGING ALONG SUNSET ROAD, FORT EXAMPLE, FL, SHE WAS APPROACHED BY SGT JOHNSON, WHO WAS TRAVELING IN HIS PRIVATELY OWNED VEHICLE (POV) AND HAD PULLED UP BESIDE HER. SGT ARLINGTON ADDED THAT SHE AND SGT JOHNSON THEN SAT IN HIS POV AND, WHILE ENGAGED IN CONVERSATION, HE

PHYSICALLY FORCED HER INTO THE REAR SEAT, REMOVED HER RUNNING SHORTS, AND FORCED HER TO ENGAGE IN SEXUAL INTERCOURSE. SGT ARLINGTON ADDED THAT FEARING SHE COULD GET HURT, SHE DID NOT PHYSICALLY RESIST SGT JOHNSON; HOWEVER, SHE DID MAKE IT CLEAR THAT SHE DID NOT WANT TO ENGAGE IN SEXUAL INTERCOURSE WITH HIM. AFTER THE INCIDENT, SGT JONHSON AGREED TO DRIVE SGT ARLINGTON BACK TO HER RESIDENCE, AFTER SHE ASSURED HIM SHE WOULD NOT MAKE A COMPLAINT. UPON ARRIVING AT HER RESIDENCE (ON-POST BARRACKS), SGT ARLINGTON NOTIFIED THE MILITARY POLICE.

AT 1630, 10 JAN 99, SGT JOHNSON WAS ADVISED OF HIS RIGHTS AND INTERVIEWED. DURING HIS INTERVIEW, SGT JOHNSON RENDERED A SWORN STATEMENT IN WHICH HE ADMITTED TO HAVING ENGAGED IN SEXUAL INTERCOURSE WITH SGT ARLINGTON, BUT ADDED THAT THE ENCOUNTER WAS CONSENSUAL. INVESTIGATION CONTINUES BY USACIDC.

REQUEST CRC NAME CHECK ON SGT JOHNSON AND SGT ARLINGTON.

7. COMMANDERS ARE REMINDED OF THE PROVISIONS OF AR 600-8-2 PERTAINING TO SUSPENSION OF FAVORABLE PERSONNEL ACTIONS AND AR 380-67 FOR THE SUSPENSION OF SECURITY CLEARANCES OF PERSONS UNDER INVESTIGATION.

8. CID REPORTS ARE EXEMPT FROM AUTOMATIC TERMINATION OF PROTECTIVE MARKINGS IN ACCORDANCE WITH CHAPTER 3, AR 25-55.

FOR OFFICIAL USE ONLY

Figure 7-1. Initial Report Format

Figure 7-2. Status Report Format

DATE: 26 FEB 99 11:00
FROM: SAC USACIDC RES AGCY FORT EXAMPLE FL //CIRCW-FEF//
TO: DIR USACRC USACIDC FORT BELVOIR VA //CICR-ZA//
PROVOST MARSHAL FORT EXAMPLE FL 33141
SJA FORT EXAMPLE FL 33141
CDR A COMPANY, 71ST ORD BN FORT EXAMPLE FL 33141
CDR USACIDC 2D MP BN FT STANDARD GA 22102 //CIRCW-FSG//
CDR 3RD MP GROUP (CID) FORT GILLEM GA //CIRC-ZA//
CDR USACIDC FT BELVOIR VA //CIOP-ZA//

SUBJECT: CID REPORT OF INVESTIGATION – 2D STATUS/SSI – 0002-99-CID000-00002 – 6E1E1 / 5M2 / 9G1 / 9G2

DRAFTER: HUDSON, KATHI L.
RELEASER: CANDRELLA, GUIDO

UNCLASSFIED - FOR OFFICIAL USE ONLY

1. DATES/TIMES/LOCATIONS OF OCCURRENCES:
1. 10 JAN 1999/0630 - 10 JAN 1999/0700; SUNSET ROAD, ADJACENT RANGE NUMBER 3, FORT EXAMPLE, FL 33141

2. 10 JAN 1999/1500 - 10 JAN 1999/1800; BUILDING 911 (CID OFFICE), FORT EXAMPLE, FL 33141

2. DATE/TIME REPORTED: 10 JAN 1999, 0800

3. INVESTIGATED BY: SA TAZ MONTANO, 4039; SA KATHI L. HUDSON, 4812; SA ROLLING E. HILL, 4366

4. SUBJECT: 1. JOHNSON, MATHEW WILLIAMS; SGT; 635-85-7456; 7 AUG 1979; COLUMBIA, SC; M; OTHER; A COMPANY, 71ST ORDNANCE BATTALION (A CO, 71ST ORD BN), FORT EXAMPLE, FL, 33141; TC; [RAPE (UNFOUNDED)].

[ADD] 2. ARLINGTON, MARY JANE; SGT; 864-00-7463; 20 JUN 78; MIAMI, FL; F; WHITE; A CO, 71ST ORD BN, FORT EXAMPLE, FL 33141; TC; [FALSE SWEARING].

5. VICTIM: 1. ARLINGTON, MARY JANE; SGT; 864-00-7463; 20 JUN 78; MIAMI, FL; F; WHITE; A CO, 71ST ORD BN, FORT EXAMPLE, FL 33141; TC; [RAPE (UNFOUNDED)].

[ADD] 2. U.S. GOVERNMENT, FORT EXAMPLE, FL 33141; [FALSE SWEARING].

6. INVESTIGATIVE SUMMARY: THE INFORMATION IN THIS REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY CHANGE PRIOR TO THE COMPLETION OF THE INVESTIGATION.

2D STATUS:

THIS STATUS REPORT IS BEING SUBMITTED TO UNFOUND THE OFFENSE OF RAPE, ADD SGT ARLINGTON AS A SUBJECT OF FALSE SWEARING, AND THE U.S. GOVERNMENT AS THE VICTIM OF THE SAME OFFENSE.

ON 25 FEB 99, SGT ARLINGTON WAS RE-INTERVIEWED AS A SUSPECT OF FALSE SWEARING. DURING THE COURSE OF HER INTERVIEW, SGT ARLINGTON RENDERED A SECOND SWORN STATEMENT IN WHICH SHE ADMITTED THAT HER INITIAL ALLEGATION OF RAPE WAS FALSE.

SGT ARLINGTON ADDED THAT SHE AND SGT JOHNSON HAD ENGAGED IN CONSENSUAL SEXUAL INTERCOURSE AND THAT SHE ONLY ALLEGED SHE HAD BEEN RAPED TO AVOID CONFLICT WITH HER FIANCÉ. SGT ARLINGTON ADDED THAT HER INITIAL SWORN STATEMENT WAS FALSE AND THAT SHE RENDERED THE STATEMENT KNOWING IT CONTAINED FALSE INFORMATION.

INITIAL REPORT:

THIS INVESTIGATION WAS INITIATED UPON NOTIFICATION BY THE FORT EXAMPLE MILITARY POLICE THAT SGT ARLINGTON REPORTED SGT JOHNSON HAD RAPED HER.

ON 10 JAN 99, SGT ARLINGTON REPORTED THAT WHILE JOGGING ALONG SUNSET ROAD, FORT EXAMPLE, FL, SHE WAS APPROACHED BY SGT JOHNSON, WHO WAS TRAVELING IN HIS PRIATELY OWNED VEHICLE (POV) AND HAD PULLED UP BESIDE HER. SGT ARLINGTON ADDED THAT SHE AND SGT JOHNSON THEN SAT IN HIS POV AND, WHILE ENGAGED IN CONVERSATION, HE PHYSICALLY FORCED HER INTO THE REAR SEAT, REMOVED HER RUNNING SHORTS, AND FORCED HER TO ENGAGE IN SEXUAL INTERCOURSE. SGT ARLINGTON ADDED THAT FEARING SHE COULD GET HURT, SHE DID NOT PHYSICALLY RESIST SGT JOHNSON; HOWEVER, SHE DID MAKE IT CLEAR THAT SHE DID NOT WANT TO ENGAGE IN SEXUAL INTERCOURSE WITH HIM. AFTER THE INCIDENT, SGT JONHSON AGREED TO DRIVE SGT ARLINGTON BACK TO HER RESIDENCE, AFTER SHE ASSURED HIM SHE WOULD NOT MAKE A COMPLAINT. UPON ARRIVING AT HER RESIDENCE (ON-POST BARRACKS), SGT ARLINGTON NOTIFIED THE MILITARY POLICE.
AT 1630, 10 JAN 99, SGT JOHNSON WAS ADVISED OF HIS RIGHTS AND INTERVIEWED. DURING HIS INTERVIEW, SGT JOHNSON RENDERED A SWORN STATEMENT IN WHICH HE ADMITTED TO HAVING ENGAGED IN SEXUAL INTERCOURSE WITH SGT ARLINGTON, BUT ADDED THAT THE ENCOUNTER WAS CONSENSUAL. INVESTIGATION CONTINUES BY USACIDC.

7. COMMANDERS ARE REMINDED OF THE PROVISIONS OF AR 600-8-2 PERTAINING TO SUSPENSION OF FAVORABLE PERSONNEL ACTIONS AND AR

380-67 FOR THE SUSPENSION OF SECURITY CLEARANCES OF PERSONS UNDER INVESTIGATION.

8. CID REPORTS ARE EXEMPT FROM AUTOMATIC TERMINATION OF PROTECTIVE MARKINGS IN ACCORDANCE WITH CHAPTER 3, AR 25-55.

FOR OFFICIAL USE ONLY

Figure 7-2. Status Report Format

Figure 7-3. Final Report Format

DEPARTMENT OF THE ARMY
1ST MILITARY POLICE DETACHMENT, CASE (CID)
3RD MILITARY POLICE GROUP, USACIDC
FORT EXAMPLE, FLORIDA 33141-5000

CIOP-OP (195) 01 May 1999

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: CID REPORT OF INVESTIGATION - FINAL - 0002-99-CID000-00002 - 6E1E1 / 5M2 / 9G1 / 9G2

DATES/TIMES/LOCATIONS OF OCCURRENCES:
1. 10 Jan 1999/0630 - 10 Jan 1999/0700; SUNSET ROAD, ADJACENT RANGE NUMBER 3, FORT EXAMPLE, FL 33141

2. 10 Jan 1999/1500 - 10 Jan 1999/1800; BUILDING 911 (CID OFFICE), FORT EXAMPLE, FL 33141

DATE/TIME REPORTED: 10 Jan 1999, 0800

INVESTIGATED BY: SA TAZ MONTANO, 4039; SA KATHI L. HUDSON, 4812; SA ROLLING E. HILL, 4366

SUBJECT: 1. JOHNSON, MATHEW WILLIAMS; SGT; 635-85-7456; 7 AUG 1979; COLUMBIA, SC; M; OTHER; A COMPANY, 71ST ORDNANCE BATTALION (A CO, 71ST ORD BN), FORT EXAMPLE, FL, 33141; [RAPE (UNFOUNDED)].

2. ARLINGTON, MARY JANE; SGT; 864-00-7463; 20 JUN 78; MIAMI, FL; F; WHITE; A CO, 71ST ORD BN, FORT EXAMPLE, FL 33141; [FALSE SWEARING].

VICTIM: 1. ARLINGTON, MARY JANE; SGT; 864-00-7463; 20 JUN 78; MIAMI, FL; F; WHITE; A CO, 71ST ORD BN, FORT EXAMPLE, FL 33141; [RAPE (UNFOUNDED)].

2. U.S. GOVERNMENT, FORT EXAMPLE, FL 33141; [FALSE SWEARING].

FOR OFFICIAL USE ONLY

INVESTIGATIVE SUMMARY: On 10 Jan 99, SGT ARLINGTON reported that while jogging along Sunset Road, Fort Example FL, she was approached by SGT JOHNSON, who was traveling in his privately owned vehicle (POV) and had pulled up beside her. SGT ARLINGTON added that she and SGT JOHNSON then sat in his POV and, while engaged in conversation, he physically forced her into the rear seat, removed her running shorts, and forced her to engage in sexual intercourse. SGT ARLINGTON added that fearing she could get hurt, she did not physically resist SGT JOHNSON; however, she did make it clear that she did not want to engage in sexual intercourse with him. After the incident, SGT JOHNSON dropped her off at her quarters. SGT ARLINGTON subsequently notified the military police.

The conduct of this investigation determined that SGT JOHNSON did not commit the offense of Rape, as originally reported by SGT ARLINGTON, in that the reported sexual contact was consensual. Investigation established probable cause to believe that SGT ARLINGTON committed the offense of False Swearing when she, after reporting that she had been raped by SGT JOHNSON, rendered a sworn statement which she knew to be false.

STATUTES:

Article 107, UCMJ: False Swearing
Article 120, UCMJ: Rape (Unfounded)

EXHIBITS/SUBSTANTIATION:

Attached:

1. Agent's Investigative Report (AIR) of SA HUDSON, 11 Jan 99, detailing his receipt of the initial complaint, initial interview of SGT ARLINGTON, interview of her attending physician; Dr. (LTC) ANDREWS, and the seizure of sexual assault protocols and soiled clothing of SGT ARLINGTON and SGT JOHNSON.

2. (2-1/2-2) Medical examination reports concerning SGT ARLINGTON and SGT JOHNSON, 10 Jan 99, detailing the lack of internal injuries to SGT ARLINGTON and the collection of sexual assault protocols from SGT ARLINGTON and SGT JOHNSON.

3. AIR of SA MONTANO, 12 Jan 99, detailing the crime scene examination and bilingual interview of Mr. ALVAREZ, and oral interview of Mr. GALLOWAY in which he related how SGT ARLINGTON told him she was raped by SGT JOHNSON.

4. Crime Scene Sketch, 12 Jan 99, prepared by SA MONTANO.

5. English language translation of Mr. ALVAREZ's statement, Exhibit 14, translated by SA MONTANO.

6. AIR of SA HILL, 12 Jan 99, detailing the suspect interview of SGT JOHNSON and formal interview of SGT ARLINGTON.

7. Waiver Certificate and Sworn Statement of SGT JOHNSON, 10 Jan 99, in which he admitted that he and SGT ARLINGTON engaged in sexual intercourse, but stated that the encounter was consensual.

8. Sworn Statement of SGT ARLINGTON, 10 Jan 99, in which she related how she was confronted by SGT JOHNSON and forced to engage in sexual intercourse with him.

9. U.S. Army Criminal Investigation Laboratory Examination Report, 99-CID131-0047, 18 Feb 99, reporting that an examination of the submitted clothing did not result in the recovery of any serological evidence.

10. Waiver Certificate of SGT JOHNSON, 24 Feb 99.

11. Polygraph report (SGT JOHNSON), 24 Feb 99, documenting SGT JOHNSON's insistence that his sexual encounter with SGT ARLINGTON was consensual.

12. AIR of SA HUDSON, 25 Feb 99, detailing the suspect interview of SGT ARLINGTON and coordination with SJA.

13. Waiver Certificate and Sworn Statement of SGT ARLINGTON, 25 Feb 99, in which she admitted that she and SGT JOHNSON had engaged in consensual sexual intercourse and that her initial sworn statement was false and that she had claimed she was raped to avoid further arguments with her fiancé.

14. Spanish language statement of Mr. ALVAREZ, 12 Jan 99, relating that he was the ground's keeper for Range Number 3 and that he did see two people by the wood line, but did not believe their encounter was confrontational (USACRC and file only).

15. Photographic packet comprised of 6 photographs (photographs 38-43). (Minor injuries of SGT ARLINGTON).

16. Photographic negatives (originals) of Exhibit 15 (USACRC only).

17. Photographic packet comprised of 37 photographs.

a. Packet containing photographs 1-20 (crime scene).

b. Packet containing photographs 21-37 (crime scene).

18. Compact disc 990001.101 containing all photographic images and the originals of Exhibit 17 (USACRC copy only).

19. Crime Lab Examination Request, 14 Jan 99, requesting that the clothing of both SGT ARLINGTON and SGT JOHNSON be examined to determine if either contained fluids which could determine if they engaged in sexual activities with each other (USACRC and file only).

20. (20-1 through 20-4) DA Form 4137, Evidence/Property Custody Document, vouchers (VO) 022-99, 023-99, 024-99 and 025-99, 11 Jan 99.

Not Attached:

Retained in the evidence depository, this office:

21. Sexual assault protocol (SGT ARLINGTON), VO 022-99.

22. One pair of gray sweat pants (SGT ARLINGTON), VO 023-99.

23. One "Army" gray T-shirt (SGT ARLINGTON), VO 023-99.

24. One pair of soiled red panties (SGT ARLINGTON), VO 023-99.

25. Sexual assault protocol (SGT JOHNSON), VO 024-99.

26. One paid of blue sweat pants (SGT JOHNSON), VO 025-99.

27. One blue T-shirt (SGT JOHNSON), VO 025-99.

28. One pair of soiled white "jockey" shorts (SGT JOHNSON), VO 025-99.

Retained in the files of the U.S. Army Crime Records Center, Fort Belvoir, VA:

29. Polygraph Authorization (SGT JOHNSON), 23 Feb 99.

30. Polygraph Examination Statement of Consent (SGT JOHNSON), 24 Feb 99.

31. Four Polygraph Charts (SGT JOHNSON), 24 Feb 99.

The originals of Exhibits 1 through 7, 9 through 12, and 14 are attached to the USACRC copy of this report. The original of Exhibits 8 and 13 are retained in the files of this office, pending adjudication. The original of Exhibit 19 is retained in the files of the U.S. Army Criminal Investigation Laboratory, Forrest Park, GA 30297-5122. The originals of Exhibit 20 are retained in the files of the evidence depository, this office.

STATUS: This is a final report. Commander's Report of Disciplinary Action Taken (DA Form 4833) is pending.

Report Prepared By:	Report Approved By:
KATHI L. HUDSON Special Agent, 3812	GUIDO CANDRELLA Special Agent in Charge

DISTRIBUTION:

1 - DIR, USACRC (original), Fort Belvoir, VA 22060
1 - Action Commander:
THRU: CDR, 71st Ord Bn, Fort Example, FL 33141
TO: CDR, A Co, 71st Ord Bn, Fort Example, FL 33141
1 - THRU:
CDR, 3rd MP Group, USACIDC, Fort Gillem, GA
CDR, 2nd MP Bn, USACIDC, Fort Standard, GA 22102
TO: CDR, USACIDC (ATTN: CIOP-CO), Fort Belvoir, VA 22060
1 - SJA (ATTN: CPT MITCHEM), Fort Example, FL 33141
1 - PMO (ATTN: MPR 00001-99), Fort Example, FL 33141 (e-mail)
1 - File

Figure 7-4. Interim Report Memorandum

Figure 7-5. 1st Supplemental Report Format

DATE: 25 DEC 98 1300
FROM: SAC USACIDC RES AGCY FORT BELVOIR VA //CIRCW-RFB//
TO: DIR USACRC USACIDC FORT BELVOIR VA //CICR-ZA//
PROVOST MARSHAL FORT BELVOIR VA 22060
SJA FORT BELVOIR VA 22060
CDR B COMPANY, 20TH ENG BN FORT BELVOIR VA 22060
CDR USACIDC WASHINGTON DIST FORT MYER VA //CIRCW-ZA//
CDR 3RD MP GROUP (CID) FORT GILLEM GA //CIRC-ZA//

SUBJECT: CID REPORT OF INVESTIGATION - 1ST SUPPLEMENTAL - 0001-98-CID122-00001 - 7G1B1 / 7C2A / 5X1

DRAFTER: WOODMAN, WOODY
RELEASER: FURR, FUZZY

UNCLASSIFIED - FOR OFFICIAL USE ONLY

1. DATES/TIMES/LOCATIONS OF OCCURRENCES:
1. 30 OCT 1998/1910 - 2110, ROOM 311, BUILDING 101, COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060

2. 24 NOV 98/1400, FORT BELVOIR RESIDENT AGENCY, 3D MILITARY POLICE GROUP (CID) USACIDC, 6007 PARK ROAD, SUITE 101, FORT BELVOIR, VA 22060-5269

2. DATE/TIME REPORTED: 31 OCT 1998, 1130

3. INVESTIGATED BY: SA WOODY WOODMAN, 1212

4. SUBJECT: 1. JONES, PAUL DONALD; SGT; 202-02-0002; 29 MAR 1971; STAFFORD, VA; M; WHITE; COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060; FC; [LARCENY] [CONSPIRACY] [HOUSEBREAKING (UNFOUNDED)] [FALSE SWEARING].

2. THOMPSON, JACK ANDREWS; SPC; 404-44-4440; 2 DEC 1973; FALLS CHURCH, VA; M; OTHER; COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060; FC; [LARCENY (UNFOUNDED)] [CONSPIRACY (UNFOUNDED)].

ADD: 3. MITCHEM, ALBERT PAUL; SPC; 265-84-9374; 1 JUL 1979, MIAMI, FL; M; BLACK; COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060; FC; [LARCENY] [CONSPIRACY].

5. VICTIM: 1. SMITH, THOMAS (NMN); SPC; 001-11-0011; 29 FEB 1972; JOHNSTOWN, PA; M; BLACK; COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060; FC; [LARCENY] [CONSPIRACY] [HOUSEBREAKING (UNFOUNDED)].

2. U.S. GOVERNMENT, (COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060); [HOUSEBREAKING (UNFOUNDED)] [CONSPIRACY].

ADD: 3. U.S. GOVERNMENT, FORT BELVOIR, VA 22060-5269; [FALSE SWEARING].

6. INVESTIGATIVE SUMMARY: THE INFORMATION IN THIS REPORT IS BASED UPON AN ALLEGATION OR PRELIMINARY INVESTIGATION AND MAY CHANGE PRIOR TO THE COMPLETION OF THE INVESTIGATION.

1ST SUPPLEMENTAL:

THIS SUPPLEMENTAL REPORT IS BEING SUBMITTED TO ADD SPC MITCHEM AS A SUBJECT OF THIS INVESTIGATION, TO ADD THE US GOVERNMENT AS A VICTIM, RE-FOUNDING THE OFFENSE OF CONSPIRACY, AND TO ADD THE OFFENSE OF FALSE SWEARING.

AT 1100, 23 DEC 98, SGT JONES WAS RE-ADVISED OF HIS RIGHTS, WHICH HE WAIVED, AND REPORTED TO THE FORT BELVOIR CID OFFICE THAT WHEN HE WAS INITIALLY INTERVIEWED ON 24 NOV 98, HE PROVIDED A SWORN STATEMENT HE KNEW WAS FALSE. SGT JONES ADDED THAT WHEN HE STOLE SPC SMITH'S TELEVISION AND VIDEOCASSETTE RECORDER, SPC MITCHEM ASSISTED HIM BY SUGGESTING THAT HE SELL THE PROPERTY AT A PAWNSHOP. SGT JONES ADDED THAT MITCHEM RECEIVED $70.00 FOR HIS SERVICES.

AT 1400, 23 DEC 98, SPC MITCHEM WAS ADVISED OF HIS RIGHTS AND INTERVIEWED. SPC MITCHEM RENDERED A STATEMENT IN WHICH HE ADMITTED TO KNOWING THAT SGT JONES HAD STOLEN SPC SMITH'S PROPERTY, THAT HE SUGGESTED SGT JONES SELL THE PROPERTY AT A PAWNSHOP, AND THAT HE RECEIVED $70.00 FOR HIS INVOLVEMENT.

FINAL REPORT:

INVESTIGATION ESTABLISHED PROBABLE CAUSE TO BELIEVE THAT SGT JONES COMMITTED THE OFFENSE OF LARCENY WHEN HE STOLE NUMEROUS ITEMS OF SPC SMITH’S PROPERTY, COLLECTIVELY VALUED AT $2,400.00, AND SUBSEQUENTLY PAWNED THE ITEMS AT THE ABC PAWNSHOP, 111 SOUTH CENTRAL STREET, STAFFORD, VA 22554. SGT JONES, A ROOMMATE OF SPC SMITH, DID NOT UNLAWFULLY ENTER THEIR ROOM WHEN STEALING THE ITEMS, THEREFORE, THE OFFENSE OF HOUSEBREAKING IS UNFOUNDED.

INVESTIGATION ALSO DISCLOSED SPC THOMPSON DID NOT KNOWINGLY PARTICIPATE IN THE THEFT AND DID NOT CONSPIRE WITH SGT JONES TO STEAL THE ITEMS. SGT JONES SOLICITED SPC THOMPSON'S ASSISTANCE IN CARRYING THE ITEMS FROM THE ROOM UNDER THE PRETENSE THE ITEMS WERE BEING TAKEN FOR REPAIR. THEREFORE, THE OFFENSE OF CONSPIRACY IS ALSO UNFOUNDED.

INVESTIGATION CONTINUES BY THE USACIDC.

7. COMMANDERS ARE REMINDED OF THE PROVISIONS OF AR 600-8-2 PERTAINING TO SUSPENSION OF FAVORABLE PERSONNEL ACTIONS AND AR 380-67 FOR THE SUSPENSION OF SECURITY CLEARANCES OF PERSONS UNDER INVESTIGATION.

8. CID REPORTS ARE EXEMPT FROM AUTOMATIC TERMINATION OF PROTECTIVE MARKINGS IN ACCORDANCE WITH CHAPTER 3, AR 25-55.

FOR OFFICIAL USE ONLY

Figure 7-5. 1st Supplemental Report Format

Figure 7-6. 2nd Supplemental Report Format

DEPARTMENT OF THE ARMY
FORT BELVOIR RESIDENT AGENCY
3D MILITARY POLICE GROUP (CID) USACIDC
6007 PARK ROAD SUITE 101
FORT BELVOIR, VA 22060-5269

CIRCW-RFB (195-2b) 9 Jan 1999

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: CID REPORT OF INVESTIGATION - 2D SUPPLEMENTAL - 0001-98-CID122-00001 - 7G1B1 / 7C2A / 5X1

DATES/TIMES/LOCATIONS OF OCCURRENCES:

1. 30 OCT 1998/1910 - 2110, ROOM 311, BUILDING 101,COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060

2. 24 NOV 98/1400, FORT BELVOIR RESIDENT AGENCY, 3D MILITARY POLICE GROUP (CID) USACIDC, 6007 PARK ROAD SUITE 101, FORT BELVOIR, VA 22060-5269

DATE/TIME REPORTED: 31 OCT 1998, 1130

INVESTIGATED BY: SA WOODY WOODMAN, 1212

SUBJECT: 1. JONES, PAUL DONALD; SGT; 202-02-0002; 29 MAR 1971; STAFFORD, VA; M; WHITE; COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060; [LARCENY] [CONSPIRACY] [HOUSEBREAKING (UNFOUNDED)] [FALSE SWEARING].

2. THOMPSON, JACK ANDREWS; SPC; 404-44-4440; 2 DEC 1973; FALLS CHURCH, VA; M; OTHER; COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060; [LARCENY (UNFOUNDED)] [CONSPIRACY (UNFOUNDED)].

3. MITCHEM, ALBERT PAUL; SPC; 265-84-9374; 1 JUL 79, MIAMI, FL; M; BLACK; COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060; [LARCENY] [CONSPIRACY].

FOR OFFICIAL USE ONLY

VICTIM: 1. SMITH, THOMAS (NMN); SPC; 001-11-0011; 29 FEB 1972; JOHNSTOWN, PA; M; BLACK; COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060; [LARCENY] [CONSPIRACY] [HOUSEBREAKING (UNFOUNDED)].

2. U.S. GOVERNMENT, (COMPANY B, 20TH ENG BN, FORT BELVOIR, VA 22060); [HOUSEBREAKING (UNFOUNDED)].

3. U.S. GOVERNMENT, FORT BELVOIR, VA 22060-5269); [FALSE SWEARING].

INVESTIGATIVE SUMMARY: At 1030, 31 Oct 98, SPC SMITH reported to the Military Police that his television and videocassette recorder were stolen from his room. In a subsequent written statement, SPC SMITH related he suspected his roommate, SGT JONES, of the theft because SGT JONES was experiencing significant financial problems.

Investigation established probable cause to believe that SGT JONES committed the offense of Larceny when he stole numerous items of SPC SMITH’s property, collectively valued at $2,400.00, and subsequently pawned the items at the ABC Pawnshop, 111 South Central Street, Stafford, VA 22554. SGT JONES, a roommate of SPC SMITH, did not unlawfully enter their room, therefore, the offense of Housebreaking is unfounded.

Investigation also disclosed that SPC THOMPSON did not knowingly participate in the theft and did not conspire with SGT JONES to steal the items. SGT JONES solicited SPC THOMPSON's assistance in carrying the items from the room under the pretense the items were being taken for repair.

Further investigation disclosed SPC MITCHEM committed the offense of Larceny when he assisted SGT JONES in stealing SPC SMITH's property by suggesting that SGT JONES sell the property at the ABC Pawnshop. SPC MITCHEM received $70.00 for his assistance. SGT JONES and SPC MITCHEM also committed the offense of Conspiracy, as both acted in concert in the theft of SPC SMITH's property. SGT JONES also committed the offense of False Swearing when, during his initial interview, he rendered a sworn statement he knew to be false.

STATUTES:

ARTICLE 121, UCMJ, LARCENY
ARTICLE 81, UCMJ, CONSPIRACY
ARTICLE 130, UCMJ, HOUSEBREAKING (UNFOUNDED)
ARTICLE 134, UCMJ, FALSE SWEARING

EXHIBITS:

ADDED ATTACHED:

16. Agent Investigation Report by SA WOODMAN, 3 Dec 98, detailing the re-interview of SGT JONES, interview of SPC MITCHEM, and additional SJA coordination.

17. Rights Waiver Certificate and Sworn Statement, 23 Dec 98, of SGT JONES admitting to rendering a false statement and describing SPC MITCHEM's involvement in the theft.

18. Rights Waiver Certificate and Sworn Statement of SPC MITCHEM, 23 Dec 98, during which he admitted that he suggested SGT JONES pawn SPC SMITH’s property and received $70.00 for his assistance.

ADDED NOT ATTACHED:

None

The originals of exhibits 16 through 18 are retained in the files of this office (pending Commander's action).

STATUS: This is a 2nd Supplemental Report. Commander's Report of Action (DA Form 4833) is pending.

Report Prepared By:

WOODY WOODMAN
Special Agent, 1212

Report Approved By:

FUZZY FURR
Special Agent in Charge

DISTRIBUTION:

1 USACRC (Original)
1 Thru: Washington District, USACIDC
To: Ops, 3rd MP Group (CID)
1 Action Commander, B Company, 20th Engineer Bn
1 Provost Marshal, MPR # 0001-98-MPC122 (Less Exhibits)
1 SJA
1 File

Figure 7-7. Agent's Investigative Report (Non-Form)

1ST MILITARY POLICE DETACHMENT, CASE (CID), 3RD MILITARY POLICE GROUP, USACIDC, FORT EXAMPLE, FL 33141-5000

AGENT'S INVESTIGATIVE REPORT
0002-99-CID000-00002
12 JAN 99

DETAILS:

At 1630 10 Jan 99, SA HILL advised SGT Matthew W. JOHNSON, 635-85-7456, A Co, 71st Ord Bn, Fort Example, FL 33141, of his rights, which he waived. During his interview, JOHNSON rendered a written statement in which he related that he and SGT ARLINGTON did engage in sexual intercourse, but he added that it was consensual. (See Waiver Certificate and Statement of SGT JOHNSON for details.)

At 1745, 10 Jan 99, SGT JOHNSON was fingerprinted, photographed, and released to his unit.

At 1820, 10 Jan 99, SGT ARLINGTON was re-interviewed. During her interview, her oral statement to SA HUDSON was reduced to writing in the form of a sworn statement. (See Statement of SGT ARLINGTON for details).

At 1915, 10 Jan 99, the undersigned exposed photographs of several small bruises located on SGT ARLINGTON's right and left upper arms. Photographs were taken with a Canon AE-1, 35mm camera, 50mm macro lens, and Kodak 200 ASA color film. ///LAST ENTRY///

Figure 7-7. Agent's Investigative Report (Non-Form)

Figure 7-8. Agent's Investigative Report (Form)

Figure 7-8. Agent's Investigative Report (Form)

Figure 7-9. Agent's Investigative Report (Form)

Figure 7-9. Agent's Investigative Report (Form)

Figure 7-10. Agent's Activity Summary

Figure 7-10. Agent's Activity Summary

Figure 7-11. Internal USACIDC Memorandum for Record

CIOP-COP 5 Mar 1999

MEMORANDUM FOR RECORD

SUBJECT: WARNING - USACIDC Channels Only - Polygraph information; SGT Mary J. ARLINGTON, 635-85-7456, A Co, 71st Ord Bn, Fort Example, FL 33141 (ROI: 0002-99-CID000-00002)

1. On 25 Feb 99, SGT ARLINGTON was afforded the opportunity to undergo polygraph testing. SGT ARLINGTON declined the offer, stating that her attorney advised her against taking a polygraph.

2. Point of contact for this memorandum is the undersigned, DSN: 656-0224.

KATHI L. HUDSON
Special Agent, 4812

DISTRIBUTION:

1 - DIR, USACRC, Fort Belvoir, VA 22060
1 - CDR, 2nd MP Det, USACIDC, Fort Standard, GA 22102
1 - File

Figure 7-11. Internal USACIDC Memorandum for Record

Figure 7-12. CID Form 14, Document Cover Sheet

Figure 7-12. CID Form 14, Document Cover Sheet

Figure 7-13. DA Form 4833, Commander's Report of Disciplinary or Administrative Action

Figure 7-13. DA Form 4833, Commander's Report of Disciplinary or Administrative Action

CHAPTER 8

8-1
General

a. This chapter provides routine and special distribution schemes and specifies restrictions on distribution in certain instances. Chapter 25 provides detailed guidance concerning authorized disclosures.

b. The dissemination of criminal investigative information must be severely limited and closely controlled. Dissemination of personal information arising from criminal investigations is permissible only when:

(1) The recipient has a need for information contained in the record in the performance of official duties, the use is compatible with the purposes for which the record is maintained, and release is not prohibited by law or policy.

(2) Release is required by law.

8-2
Variances

a. A CID supervisor may permit additional distribution as needed, provided adherence is made to the overriding restrictions in paragraph 8-1.

b. A USACIDC supervisor may restrict distribution in conformity with AR 195-2. In such cases, an additional paragraph will state that distribution of the report is being restricted to USACIDC channels and provide a brief statement of the reason(s) for the restriction (e.g., “RESTRICTED DISTRIBUTION: Due to the covert nature of this investigation, distribution of this report is restricted to USACIDC channels only.”). All subsequent status/supplemental reports will contain this paragraph, until the distribution restriction is no longer required at which time a status/supplemental report will be initiated lifting the restricted distribution (e.g., "RESTRICTED DISTRIBUTION: Distribution of this report is no longer restricted to USACIDC channels."). Refer to Chapter 7 of this regulation for further guidance.

Note: Commanders and supervisors at all levels should make judicious use of this feature because it conflicts with one of the purposes of the DCII which is to ensure DoD investigative agencies are aware when other offices are investigating someone or some entity. Accordingly, the restriction should be removed as soon as possible.

c. If requested and a valid need exists, distribution may be made to the commander of individuals or units listed as victims in the report of investigation. Routine distribution to these commanders is not authorized.

d. A copy of each report of investigation (initial, status, final and supplemental), in which an AAFES activity is listed as a victim, will be provided to AAFES in accordance with the distribution cited in paragraph 8-28.

e. Reports of investigation which contain IG reports/documents/information require special handling in accordance with AR 20-1. Such documents or information will not be released outside USACIDC channels. Requests for exception will be forwarded to DAIG-ZXR, Washington, DC 20310.

f. National Guard & Reserves

(1) For investigations involving the personnel or property of the Army National Guard, the action commander will be the state adjutant general.

(2) For investigations involving personnel or property of the USAR, the action commander will be the appropriate ARCOM or GOCOM commander.

(3) The provisions of paragraph 8-10e do not apply to paragraphs 8-2f(1) and (2).

g. One complete copy of all final death investigations and final command monitored ROIs is required to be forward to the Commander, USACIDC, ATTN: CIOP-COP-CO. These are the only final ROIs required to be forwarded to HQUSACIDC on a routine basis. A copy of all initial SSI, status SSI and SSI Only reports are required to be forwarded to HQUSACIDC.

8-3
General

The distribution shown in this section will be routinely accomplished for all reports of investigation (initial, status, final, etc.). When distributing unfounded cases, exhibits will normally be attached only to the action commander, file and Crime Records Center copies of the report. All death investigation cases will include copies of exhibits with the AFIP copy of the report. The limitation of exhibits to only certain copies of the report will be identified as required by paragraph 7-14m(1).

8-4
Original

The original of all final, referred, collateral, and supplemental reports of investigation, will be forwarded to:

Director
U.S. Army Crime Records Center
ATTN: CICR-CR
6010 6th Street
Fort Belvoir, VA 22060-5506.

8-5
File copy

One copy of all reports of investigation will be retained in the case folder of the preparing USACIDC unit (for branch offices, the completed case folder will be retained by the parent unit).

8-6
Intermediate USACIDC headquarters

Requirements for forwarding copies of reports of investigation to the USACIDC major subordinate command will be established by the USACIDC major subordinate commander.

8-7
Other USACIDC elements

When complaints are received concerning incidents which occurred within the area of responsibility of another USACIDC major subordinate command, an information copy of each report of investigation (initial, SSI, final, etc.) prepared will be provided to the USACIDC element responsible for the area in which the incident occurred.

8-8
Provost Marshal

a. One copy of each report of investigation, less exhibits (unless specifically requested by the provost marshal), will be forwarded to the provost marshal responsible for the area where the incident occurred.

b. If the incidents reported in the report of investigation occurred in the areas of responsibility of more than one provost marshal, a copy will be sent to each.

c. This distribution may be limited to specified categories of cases by local agreement between the CID supervisor and the supported provost marshal.

8-9
General

In addition to routine distribution, special distribution is required when there is an identified subject.

8-10
Supported commander/supervisor

a. One copy of each report of investigation, in which there is an identified military or DoD civilian employee subject, will be forwarded to the action commander (i.e., the company/battery/troop commander, or similar supervisor of the subject).

b. For military family members, the action commander is the installation or community commander or a designated representative.

c. When a civilian not affiliated with DoD is the subject of a report of investigation, the action commander will be the installation or community commander or a designated representative. A copy of the final report of investigation may be provided, upon request, to local, state, federal, or foreign investigative agencies. See AR 27-40 and Privacy Act accounting requirements in Chapter 21. CID Form 118-E-R (Disclosure Accounting Record) must be prepared and forwarded as directed by that regulation.

d. When there are multiple action commanders, copies will be forwarded to each.

e. Final, collateral, and supplemental reports of investigation will be forwarded to action commanders through the next higher headquarters having a field grade commander.

8-11
Staff Judge Advocate (SJA)

a. One copy of each report of investigation in which there is an identified subject will be forwarded to the SJA who supports each action commander.

b. This distribution may be limited by local agreement to specified categories of cases.

8-12
USAREC LNO

One copy of each report of investigation, in which a member of the United States Army Recruiting Command (USAREC) is identified as a subject, will be forwarded to:

USAREC LNO,
280th MP Detachment (CID)
488 Old Ironside Ave
Fort Knox, KY 40121-5580

8-13
Transients

When a subject is in a transient status, the action commander's copy of the report of investigation will be forwarded as follows:

a. In the United States. To the gaining unit commander through the supporting USACIDC unit.

b. Outside the United States. To the USACIDC office supporting the subject's new unit. If this cannot be determined at the local level, the USACIDC major subordinate command supporting the gaining unit should be contacted to determine the permanent assignment of the individual. This query will contain the following information: CID report of investigation number; full name, rank and SSAN; replacement unit; reporting date; and numbers of days leave to be taken prior to arriving at the replacement unit. The USACIDC major subordinate command receiving these inquiries will determine and verify permanent assignment and will respond to the requesting unit within five working days. The requesting USACIDC element should then send the final report of investigation directly to the CID element cited in the USACIDC major subordinate command reply.

8-14
Fugitive deserters

a. When a subject of a final report of investigation, against whom action has not been taken, is dropped from the rolls as a deserter, the USACIDC unit investigating the case will submit a copy of the report of investigation with a memorandum of transmittal to:

Director
U.S. Army Crime Records Center
6010 6th Street
Fort Belvoir, VA 22060-05506

The memorandum of transmittal will state that the subject is in a deserter status, giving the date, unit, and place of desertion and will include one legible copy of the original DD Form 553 (Deserter/Absentee wanted by the Armed Forces) and one legible copy of the original DA Form 4187 (Personnel Action) as enclosures to the report of investigation. The CRC will monitor the deserter subject's return to military control.

b. If more than one subject in a report of investigation has deserted, an action copy for each deserter subject of the report of investigation will be provided.

c. Any leads remaining to be developed upon the subject's return to military control will be fully detailed in the lead section of the report.

d. Upon receipt of a status report, or final (D) report of investigation reporting a subject as a deserter, the CRC will verify that an NCIC entry from USADIP exists, then enter the individual into the NCIC as a CID wanted fugitive.

e. All U.S. Army personnel in a deserter status, to include those listed as subjects of CID reports of investigation, are entered into the NCIC by the USADIP upon receipt of DA Form 4187 from the reporting/losing unit. The CRC cannot initiate deserter entries into the NCIC. See paragraph 5-35 for further information concerning temporary felony wants.

8-15
Death investigations

a. One copy of each initial/status report of investigation reporting a death investigation will be forwarded by the preparing element to the following message address.

DIR AFIP AFME WASH, DC//AFIP-CPLF//

b. One copy of each final/supplemental report of investigation reporting a death investigation will be forwarded by the preparing element to the following address. Exhibits previously submitted for the manner of death determination consultation do not need to be resubmitted. Photographic exhibits will be digital files, actual photographic prints or duplicated slides, not machine copies. Refer to paragraphs 5-11 and 7-14 for additional information.

Director

Armed Forces Institute of Pathology
AFIP Annex - Bldg 102
1413 Research Blvd
Rockville, MD 20858

8-16
Overseas support to U.S. Department of Justice (DOJ)

a. To determine if the United States can pursue a civil fraud remedy in a foreign court, the Civil Division, DOJ, will be immediately notified whenever a USACIDC element in an overseas area completes an investigation of any fraud or corruption case that may provide a basis for civil recovery by the United States. A copy of the final report of investigation (less exhibits) will be provided to DOJ as follows:

(1) For investigations occurring in Germany, notification will be made to:

American Embassy
24 Grosvenor SA
ATTN: Mr. James Gresser
London, WIA IAE

(2) For investigations occurring in other over-seas areas, notification will be made to:

Director
Commercial Litigation Branch
Department of Justice
Civil Division
P.O. Box 261
Ben Franklin Station
Washington, DC 20044

b. The USACIDC element controlling the investigation will independently notify the Civil Division, DOJ, irrespective of any requirement for any other reporting of the investigation within USACIDC or to OTJAG.

c. Taken collectively, paragraph 1-5g, AR 192-2; 28 U.S. Code Section 535; and paragraphs 1-4a and 1-5, AR 27-40, require that ROIs listing OCONUS DoD employees as subjects of extraterritorial Title 18 U.S. Code violations will be forwarded through channels to the HQUSACIDC SJA for possible transmittal through the Litigation Section, OTJAG, to DOJ.

8-17
Postal offenses

One copy of each final, collateral and supplemental report of investigation involving postal offenses will be forwarded through:

Commander
Military Postal Service Agency
ATTN: MPSA-OP
2461 Eisenhower Ave
Alexandria, VA 22331-0006

To:

Manager, External Liaison
Office of Criminal Investigations
U.S. Postal Inspection Service
475 L'Enfant Plaza West, SW
Washington, DC 20260-2167

8-18
Internal Revenue Service (IRS)

Within the United States, one copy of each final and supplemental report of investigation of interest to the Internal Revenue Service (e.g., illicit income from narcotics trafficking, black-marketing, etc.) will be provided upon request to the local office of the Internal Revenue Service. Outside of the U.S., a copy will be provided, upon request, to the nearest representative of the Internal Revenue Service.

8-19
Counterfeit U.S. currency

Within the United States, one copy of each final and supplemental report of investigation pertaining to counterfeit U.S. currency will be provided upon request to the local office of the U.S. Secret Service. Outside of the U.S., a copy will be provided, upon request, to the nearest representative of the U.S. Secret Service.

8-20
Defense Finance and Accounting Service (DFAS)

a. A copy of each initial, status, final and supplemental ROI involving DFAS activities will be forwarded to the installation level DFAS commander for the area in which the incident occurred and to the USACIDC-DFAS LNO at electronic mail address Ifra.cid@us.army.mil.

b. Appropriated Funds

One copy of each final, collateral, referred, and supplemental report of investigation involving the unlawful receipt of government funds will be forwarded, using a memorandum of transmittal (see figure 8-1), to the servicing Finance and Accounting Office (F&AO) for a determination of indebtedness. A copy of the memorandum and ROI will also be forwarded to regional DFAS offices at the following addresses:

For all ROI's except retirement pay:

Defense Finance & Accounting Service – Indianapolis

ATTN: DFAS-GA/IN (Office of General Counsel)
8899 East 56th Street
Indianapolis, IN 46249-0160

For all ROI's addressing retirement pay:

Defense Finance & Accounting Service - Cleveland Center

Director, Internal Review Office
ATTN: Code PI
1240 East 9th Street
Cleveland, OH 44199-2055

c. If the servicing F&AO cannot be identified, the report of investigation will be forwarded to:

Defense Finance & Accounting Service – Indianapolis
ATTN: DFAS-GA/IN (Office of General Counsel) Column 215G-1,
8899 East 56th Street
Indianapolis, IN 46249-0160

A memorandum of transmittal explaining that the servicing F&AO could not be identified will be attached.

8-21
U.S. Army commissaries

One copy of each initial, initial/SSI, status, final, collateral and supple-mental report of investigation involving U.S. Army commissaries will be sent through:

Fort Lee Resident Agency
3d MP Group, USACIDC
3800 A Ave
Fort Lee, VA 23801-6090

To:

Commander
Department of Defense Commissary Agency
1300 E Ave
ATTN: DeCA-IGF
Fort Lee, VA 23801-1800

8-22
Nonappropriated funds

One copy of each final, collateral, and supplemental report of investigation involving losses to nonappropriated fund instrumentalities (NAFI) will be provided, upon request, to the fund custodian or manager for the purpose of establishing the existence of a loss as required by AR 230-16

8-23
Child sexual abuse in DoD-sanctioned activities

One copy of each initial or initial/SSI involving an incident of child sexual abuse occurring in a DoD-sanctioned activity will be provided electronically via the Automated Criminal Investigative Reporting System (ACIRS) to the Commander, Community and Family Support Center, ATTN: CFSC-FSA, Summit Center, 4th Floor, 4700 King Street, Alexandria, VA 22302-4418, at electronic mail address:

michele.nash@cfsc.army.mil

For purposes of this regulation, a DoD-sanctioned activity is defined as a U.S. Government activity or non-governmental activity authorized by appropriate DA/DoD officials to perform childcare or supervisory functions on DoD controlled property. The care and supervision of children may be either its primary mission (e.g., child development centers, DoDEA schools, youth activities, family day care providers, etc.) or incidental in carrying out another mission (e.g., medical treatment facility).

8-24
Department of Defense Education Activity (DoDEA)

One copy of each initial, initial/SSI, status, final, and supplemental report of investigation involving DoDEA employees, the activities of DoDEA schools, or any allegation of child abuse which may involve a DoDEA employee or a DoDEA student engaged in a DoDEA sponsored activity will be furnished to:

DoDEA
Review and Compliance Office
4040 North Fairfax Drive
Arlington, VA 22203-1635

Electrical mail: dstabile@hq.odedodea.edu

8-25
Significant cases of fraud and corruption

One copy of each initial/SSI, status, final, referral, and supplemental report of investigation concerning procurement fraud cases involving an alleged loss of $100,000 or more and all corruption cases related to procurement that involve bribery, gratuities, or conflicts of interest and any procurement fraud case that has received or is expected to receive significant media coverage will be provided to:

Chief
Procurement Fraud Division
Office of the Judge Advocate General
Litigation Center
901 N. Stuart Street, Suite 500
Arlington, VA 22204-1837

8-26
Depot Systems Command (DESCOM)

One copy of each initial, status, final, and supplemental reports of investigation involving DESCOM will be forwarded to:

Special Agent-in-Charge
Carlisle Barracks Resident Agency
3d MP Group, USACIDC
116 Forbes Ave, Suit 11

Carlisle Barracks, PA 17013-5028

Message address:

SAC USACIDC RES AGCY CARLISLE BKS PA //CIRCU-RCL//

8-27
Defense Logistics Agency (DLA)

A copy of all initial, status, and final reports of investigation which involve any function or service of the DLA or any contract awarded or administered by the DLA shall be provided to the local office of the Defense Criminal Investigative Service and to:

Director
Defense Logistics Agency
ATTN: Criminal Investigation (DI) Doye Hambirck
8725 John J. Kingman, Room 3539
Fort Belvoir, VA 22060-6221

8-28
Army and Air Force Exchange Service (AAFES)

Reports of investigation involving AAFES activities will be forwarded to the installation level AAFES general manager for the area in which the incident occurred. A copy of all initial, status, final and supplemental reports will also be provided electronically via the Automated Criminal Investigative Reporting System (ACIRS) to electronic mail address:

Danishg@aafes.com

AAFES USACIDC representative, and the Fort Hood Resident Agency Liaison Officer (LNO).

8-29
U.S. Army Corps of Engineers (USACE)

In addition to other required distribution, reports of investigation pertaining to criminal allegations within the USACE will have the following distribution:

a. The action commander's copy of the CID report of investigation will be forwarded to the responsible engineer district commander.

U.S. Army Space and Missile Defense Command
1941 Jefferson Davis Hwy, Suite 900
Arlington, VA 22202

(1) Force Development & Integration Center (SMDC-IC), Arlington, VA

(2) National Missile Defense TRADOC System Manager (NMD TSM), Arlington, VA

c. The commander's action copy of the report of investigation for personnel assigned to the below listed activities will be forwarded to:

Deputy Commander
U.S. Army Space and Missile Defense Command
ATTN: SMDC-ZB
P.O. Box 1500
Huntsville, AL 35807-3801

(1) USASMDC-Huntsville, Huntsville, AL

(2) SMD Acquisition Center (SMDC-AC), Huntsville, AL

(3) Missile Defense and Space Technology Center (SMDC-TC), Huntsville, AL

(4) Space and Missile Defense Battle Lab (SMDC-BL), Huntsville, AL

(5) Army Space Program Office (SMDC-AO), Ft. Belvoir, VA

(6) High Energy Laser Systems Test Facility (SMDC-HD), White Sands Missile Range, NM

(7) JLENS Project Office (SMDC-AJ), Huntsville, AL

(8) Ballistic Missile Targets Joint Project Office (SMDC-TJ), Huntsville, AL

(9) Ballistic Systems Division Field Office, Norton Air Force Base, CA

(10) U.S. Army Boeing Field Office, Seattle, WA

(11) Lockheed-Martin Field Office, Sunnyvale, CA

(12) McDonnell-Douglas Field Office, Huntington Beach, CA

(13) Space Systems Division Field Office, Los Angeles Air Force Base, CA

(14) USASMDC Liaison Office, MIT-Lincoln Laboratory, Lexington, MA

d. Commander's action copy of the report of investigation for personnel assigned to the below listed activities will be forwarded to:

Commander
U.S. Army Kwajalein Atoll/Kwajalein Missile Range
ATTN: SMDC-KA-ZA
P.O. Box 26
APO AP 96555-2526
(1) U.S. Army Kwajalein Atoll (USAKA)

(2) Kwajalein Missile Range (SMDC-KA-R), Majuro, Republic of the Marshall Islands

(3) USAKA Field Office, Majuro, Republic of the Marshall Islands

8-34
U.S. Army Space Command (ARSPACE)

a. An information copy of each initial, status, final, and supplemental report of investigation pertaining to ARSPACE will be forwarded to:

Commander
U.S. Army Space Command
1941 Jefferson Davis Hwy, Suite 900
Arlington, VA 22202

b. The commander's action copy of the report of investigation for personnel assigned to ARSPACE (listed below) will be forwarded to:

Deputy Commander
U.S. Army Space Command
1670 N. Newport Road,
Colorado Springs, CO 80916-2749

(1) Technology Support Office (SMDC-AR-ZA-T), Colorado Springs, CO

(2) NASA Detachment (SMDC-AR-NA), Johnson Space Center, TX

(3) 1st SATCON Battalion (SMDC-AR-SB-H), Colorado Springs, CO

(4) ARSPACE European Theater Director (SMDC-AR-OE)

(5) ARSPACE JTAGS Detachment Europe (SMDC-AR-OJ-E)

(6) ARSPACE JTAGS Detachment Pacific (SMDC-AR-OJ-P)

8-35
Reports of investigation involving U.S. Army museums

One copy of each final report of investigation (less exhibits) involving U.S. Army museums will be forwarded to:

Chief of Military History
U.S. Army Center of Military History
ATTN: (DAMH-MD)
103 Third Avenue
Fort Lesley J. McNair, D.C. 20319-5058

8-36
Offenses by commercial agents

A copy of a final report of investigation involving a subject who is a commercial agent authorized to solicit on Army installations will be forwarded to:

Commander
U.S. Army Community and Family Support Center
ATTN: Installation Support Division
200 Stovall Street
Alexandria, VA 22331-0400

8-37
Military Prisoner Transfer and Assignment Criteria to the Army Correctional System.

a. Department of Defense Instruction (DoDI) 1325.7, paragraph 6.2.12, states to facilitate transfer, risk assessment, and appropriate classification of inmates, transferring commanders will ensure that the following documents accompany the prisoner: Report of investigation (ROI) (to include victim and witness statements and investigator's summary), medical records, dental records, completed victim witness forms, report of results of trial, permanent change of station orders, statement of conduct, confinement records, court-martial promulgating order, record of trial, military personnel file, and microfiche/film (restricted file).

b. To ensure compliance with DoDI 1325.7, a copy of the final ROI will be provided to the transferring commander. If the final ROI has not been completed upon the transfer of the prisoner, an interim ROI will be provided. When the

transferring commander is also the action commander, as identified in paragraph 8-10 above, and he has already been provided a final or interim ROI, another copy of the final or interim ROI need not be provided unless specially requested.

8-38
Defense Intelligence Agency (DIA)

One copy of each initial, status, collateral, final and supplemental report of investigation involving DIA personnel or activities will be electronically forwarded to **IG.Investigators@dia.mil** and **linda.freeman@dia.mil**. A hard copy of each final and supplemental ROI (w/exhibits) will be mailed to

Defense Intelligence Agency
ATTN: DIAC (Freeman, IG)
Bldg 6000
Washington, DC 20340-5100

For the purposes of this regulation DIA personnel is defined as personnel assigned to DIA elements and in the Defense Attaché System.

8-39
SSI only

SSI only reports will be provided to:

a. Commander, USACIDC, ATTN: CIOP-COP-CO.

b. Intermediate USACIDC headquarters.

c. Director, USACRC, when a name check is required.

d. The USACIDC LNO of a major command (MACOM) when the MACOM has an interest in the incident because of the location at which it occurred or the personnel involved.

(1) The USACIDC LNOs are listed at appendix E.

(2) When a USACIDC unit listed as an information addressee is the LNO for the MACOM, there is no requirement to list the USACIDC LNO.

e. The supported provost marshal.

f. The installation/community commander may be provided a copy, if appropriate.

g. Director, Armed Forces Medical Examiner //AFIP-CPLF//, AFIP Annex, Bldg 102, 1413 Research Blvd, Rockville, MD 20858 for SSI reporting deaths of any kind.

8-40
Report of Investigation (ROI) / SSI

a. When a SSI is dispatched in conjunction with an initial, status, or supplemental report of investigation, the distribution will be that of the report of investigation plus additional copies provided the Commander, USACIDC, ATTN: CIOP-COP-CO and the USACIDC LNO of the appropriate MACOM as determined in paragraph 8-39d. All exhibits supporting a SSI reportable final report of investigation meeting the requirements of paragraph 8-2g will be included with the report of investigation sent to CIOP-COP-CO.

b. Information copies of subsequent status, final, and supplemental reports of investigation will not be provided to the USACIDC LNO unless specifically requested by the LNO or prescribed by this chapter.

8-41
General

Distribution of reports of investigation and SSIs outside USACIDC channels may be withheld or delayed when warranted by operational considerations. A notation will be made in the AAS reflecting the reason for the decision to restrict or delay distribution. When restriction of distribution to CID channels only is deemed appropriate, initial, SSI and status reports also must contain the statement as reflected in paragraph 7-12m(6).

8-42
Senior personnel

When raw data, reports of investigation, or SSIs contain derogatory information about a senior person as defined in paragraph 5-4a, distribution will not be made to any person who is subordinate in position to the senior person. Special consideration should be made on how information is transmitted to preclude access by persons other than the intended recipient.

8-43
Compromise of investigative effort

If any part of the normally required distribution might compromise further investigative effort, that part of the distribution may be withheld or delayed, except within the USACIDC chain of command. When notification to a commander or provost marshal is withheld or delayed, the next higher USACIDC unit must be notified along with a higher headquarters in the chain of command of the supported commander/provost marshal at which the information may be released without impeding the investigation. Information may only be withheld from major Army commanders upon approval of the Commander, USACIDC. Requests for such approval will be directed to the Commander, USACIDC, ATTN: CIOP-COP-CO. If such a request is approved, the Commander, USACIDC, must advise the Chief of Staff, Army, or Secretary of the Army as required by paragraph 3-14a, AR 195-2.

8-44
Classified and sensitive programs

Reports of investigation and SSIs which contain classified or sensitive program information and were prepared by the Field Investigative Unit, 701st MP Group (CID), are exempt from the routine distribution requirements set forth in this chapter. Distribution will be determined on a case-by-case basis primarily dependent upon the degree of sensitivity of the information contained in the report and the need-to-know.

8-45
Normal distribution

The CPS reports will be distributed as follows:

a. The original report will be retained by the office conducting the CPS (file copy).

b. One copy with exhibits will be sent to the appropriate USACIDC major subordinate command for review and analysis.

c. One copy without exhibits will be sent by e-mail to HQUSACIDC at ciopin@belvoir.army.mil.

8-46
CPS reports distributed outside of USACID

These reports will be determined by the manner in which the CPS was initiated, i.e., a commander requested CPS or a CID directed CPS.

a. Commander requested CPS. When a commander or supervisor of an activity, facility, unit, or installation requests a CPS to assist in diagnosing the unit/activity's performance, the only external distribution of that report will be to the re questing commander for his exclusive use (action commander copy). This limited distribution is designed to encourage commanders to seek CID assistance in dealing with internal problems and to alleviate fear or concern that problems or deficiencies will be reported to their superiors, thereby causing embarrassment or increased concern by surfacing the report at higher levels. No other external distribution will be made of such reports without the expressed approval of the requesting commander. A memorandum of transmittal will be used to forward the CPS to the commander concerned.

b. A CID directed CPS. Those CPSs not requested by a commander but initiated by a CID element at any level will be considered as a CID directed CPS. External distribution of those reports will be as follows:

(1) Distribution of CPSs of Defense Logistic Agency activities will be made in accordance with AR 195-8.

(2) All CPSs of AAFES activities will be forwarded to the surveyed Army Air Force Exchange Service (AAFES) facility general manager and the AAFES USACIDC LNO.

(3) Action commander copy. One copy will be sent to the commander having responsibility for security and law enforcement for the activity/unit that received the CPS. If the activity is a tenant facility not subordinate to the local installation/activity commander, the action copy will be provided to the individual having command responsibility for the tenant activity. Information on a tenant activity that impacts upon local installation or military community will be extracted fro m the CPS and provided either verbally or by memorandum to the area provost marshal. Action commander copies of CPS reports will be forwarded using a memorandum of transmittal.

(4) Special distribution: One information copy of the report will be provided to the applicable major command or agency as needed. This is based upon the chain of command of the activity that received the CPS and whether there is a need for such distribution. For example, a CPS of a medical activity would be provided to Health Services Command, even though the activity is located on a TRADOC or FORSCOM installation. One copy to the PM who has law

enforcement jurisdiction for the activity/organization. One copy should be provided to the IG who has responsibility for the activity/organization.

(5) All mail containing investigative reports pertaining to Defense Commissary Agency (DeCA) will have the following statement on the envelope:

"TO BE OPENED BY THE DIRECTOR (COMMANDER) OR DESIGNATED REPRESENTATIVE ONLY."

(6) An information copy of all completed CPS reports will be provided to the Director, DeCA and the concerned DeCA region.

8-47
Intelligence-related Investigations

a. In additional to other required distribution, one copy of all initial, and status reports of investigation pertaining to offenses involving espionage, mishandling of classified information or equipment, sabotage, aiding the enemy, spying, as well as any joint investigation with military intelligence field operating units will be forwarded to Commander, HQ USACIDC ATTN: CIOP-ZA, via electrical message.

CHAPTER 9

9-1
Cooperation

The USACIDC units will maintain a close relationship with military police at all levels to ensure that effective investigative support is provided to the local commander.

9-2
Working relationship and supervision

a. Military police personnel as referred to in this chapter, includes General Schedule (GS) civilian grade police officers assigned duty under a provost marshal, who also may be a GS civilian.

b. When military police personnel will be participating in combined CID/MP investigative activity under the supervision of USACIDC special agents for an extended period, consideration should be given to placing the military police personnel o n special duty with the USACIDC unit. Arrangements for special duty must be agreed to by the military police unit commander and coordinated with the supporting military personnel office (MILPO). Coordination with MILPO is not required if it may compromise covert operations.

c. Military police investigators may be attached or OPCON to a USACIDC unit when approved by both the local USACIDC element and the provost marshal.

d. The USACIDC supervisors and special agents may participate in the performance evaluation of military police personnel in a special duty or attached status with a USACIDC unit. The extent of participation will be coordinated with the military police unit commander and the local MILPO.

9-3
Control of investigative situations

a. The special agent responding to a crime scene and who assumes the investigation, will take control over the scene and all persons present at the scene in accordance with AR 195-2. The special agent may utilize military police to assist in securing and processing the crime scene.

b. In a raid situation, the senior special agent responsible for planning the raid, regardless of grade of non-CID agents, will exercise supervisory responsibility over all personnel participating in the raid.

Investigative activities of the CID and MP

a. Combined CID and MP investigative activities are encouraged whenever such effort would improve the criminal investigation support provided to the supported commander. Combined activities have proven successful and mutually beneficial in the following criminal investigation activities:

(1) Drug suppression operations.

(2) Larceny investigations.

(3) Robbery investigations.

(4) Aggravated assault investigations.

(5) Criminal intelligence centers.

b. Combined investigative activities may be organized on a long-term basis, as in criminal intelligence centers and drug suppression operations, or on a short-term basis to investigate a complex crime or multiple-related crimes requiring increased and intensified investigative effort. When long-term activities are planned, the procedures will be formalized through memorandums of understanding (MOU) between the CID supervisor and the supported provost marshal. Coordination with major subordinate commands and local staff elements, such as the SJA, should also be effected.

c. In combined activities where CID/MP teams are used, the senior member of the team will be a special agent who will supervise and direct the investigative activities of all members of the team.

d. An MOU for combined investigative activities should provide for supervisory structure, commitment of personnel, continuity of personnel, operations, and when warranted, personnel evaluation reporting procedures.

e. Military police participating in combined investigative activities will not perform investigative duties for which they have received no prior training. If special training is required for military police to support a specific CID/military police operation, the training needed and/or received should be documented in writing.

9-5
Memorandum of understanding (MOU)

a. A MOU between USACIDC units and provost marshals may be used to formalize combined CID/MP investigative activities; however, an MOU to modify regulatory investigative responsibilities of CID and military police is not authorized.

b. A MOU between the CID and military police will adhere to the following paragraph format:

(1) Purpose. A brief explanation of the purpose of the MOU.

(2) Objective. A brief explanation of what is intended by the MOU.

(3) Authority. The specific paragraphs of Army, USACIDC, and local regulations which govern the MOU.

(4) Definitions (optional). A listing of definitions of terms not jointly used by the personnel affected by the MOU.

(5) Responsibilities. A listing of various responsibilities involved in the MOU and a precise determination as to whether CID or MP will be accountable. A listing of OPCON or attachment instructions.

(6) Procedures. A listing of actions which must be accomplished or which are not allowed.

(7) Coordination. The MOU must be coordinated with the installation commander, and the staff judge advocate, and any other element deemed appropriate.

(8) Expiration. This paragraph will contain the expiration date of the MOU and provisions for renewal and cancellation by either signatory.

9-6
Investigative assistance

Personnel from the USACIDC may provide assistance to the military police on investigative procedures and training in the use of investigative equipment. This assistance may also include the loan of investigative equipment. Accountability for loaned equipment will be maintained using hand receipts and the procedures in AR 710-2.

9-7
Training

USACIDC personnel may provide training for military police personnel when such participation does not interfere with USACIDC mission requirements. Military police personnel may participate in USACIDC training, when the subject material has application to their training needs.

9-8
Criminal intelligence

Military police will be permitted access to USACIDC criminal intelligence on a need-to-know basis consistent with USACIDC security requirements. Access will be controlled to ensure that information exclusively for USACIDC use is not compromised.

9-9
Controlled substances

a. Chapter 13 contains specific instructions on the conduct of USACIDC and military police drug suppression activities.

b. Although some responsibilities for investigating certain controlled substance offenses have been delegated to the military police, the USACIDC is accountable by AR 195-2 with overall responsibility for investigative activity involving controlled substances.

c. Each USACIDC unit will ensure that the military police provide prompt notification of con-trolled substance violations they are investigating as required by AR 195-2. The procedures to be followed when notified by the military police of the initiation of a controlled substance investigation are contained in chapter 13.

d. Maximum cooperation and coordination between CID and military police personnel is required in the suppression of controlled substance offenses. All USACIDC units are responsible to ensure that supported commanders are provided an effective investigative response to controlled substance problems.

9-10
Evidence

A USACIDC unit may accept military police evidence for safekeeping if a military police evidence room is not available. Such evidence will be maintained in accordance with AR 195-5.

9-11
Detention

When persons in USACIDC custody are placed in a military police detention facility, they will be detained in conformity with the policies of the local provost marshal.

9-12
Drug suppression team (DST) member

a. A drug suppression team may be comprised of military police personnel and non-military police personnel. All team member(s), whether attached to, assigned for duty with, or otherwise under USACIDC operational control for duty with a drug suppression team, will be referred to as drug suppression team member(s).

b. All CID supervisors will ensure that non-military police personnel, as well as military police and military police investigator(s), are adequately trained to execute the full responsibilities and authority of a drug suppression team member. Training must be documented in writing.

c. The district, field office, or equivalent commander, based on a recommendation of the special agent-in-charge, will determine when any individual can be certified as being properly trained to perform drug suppression operations (in writing).

d. Law enforcement procedures in connection with CID drug suppression operations such as making apprehensions, conducting searches, and interviewing suspect(s), will be performed by military police, military police investigator(s), and CID agent(s), under CID control. Non-military police personnel, who are certified as being trained, may only assist military police, military police investigator(s), and CID personnel with these type of law enforcement procedures.

CHAPTER 10

10-1
Mission

a. Logistics Security (LOGSEC) Operations

(1) LOGSEC is defined as CID efforts to enhance force protection and homeland security during peace and war through the prevention, detection and investigation of criminal acts committed by terrorist or criminal elements against the integrity of the “logistics pipeline” from the Army logistics provider to the war fighter. It includes any criminal or terrorist action directed to divert, steal, destroy, substitute or sabotage supplies delivered to, or used by, the U.S. military. The LOGSEC mission is the responsibility of all CID elements worldwide. Each echelon of CID must fulfill specific responsibilities to achieve a cohesive, effective support to the Army that enhances combat readiness. These responsibilities are further defined in the following paragraphs and in paragraph 10-6 of this regulation. The CID is the Army’s LOGSEC proponent during peace, contingency operations and war.

(2) The distinction between economic crime operations versus LOGSEC operations is often a difficult one to make. LOGSEC operations are a subpart of the larger CID mission to perform economic crime investigations that affect all operations of the Army. Pay entitlement investigations such as BAH or TDY fraud, investigations related to non-appropriated funds, or investigation of Army and Air Force Exchange Service (AAFES) fraud are examples of economic crimes that are not LOGSEC operations.

(3) CID LOGSEC operations encompass a variety of disciplines that extend beyond the conduct of criminal investigations. Effective LOGSEC support to military commanders will include crime prevention efforts, physical security examinations, LOGSEC awareness briefings, criminal intelligence collection and analysis, criminal threat assessments, and criminal vulnerability assessments. These operations are all directed toward enhancing the Army’s accountability, security and visibility of materiel, personnel, and data along the “logistics pipeline”, from the point of requirements determination through the point of materiel issue in forward deployed areas. To be effective in this endeavor, CID elements providing LOGSEC support must understand the system guiding the type of materiel being produced, transported, and distributed in their respective areas of responsibility, as well as the threat posed to the security of that materiel.

(4) The “logistics pipeline” is a term used to describe the entire continuum in which military assets are acquired, produced, transported and maintained. It includes the processes of acquisition management, materiel distribution and materiel management (including retrograde turn-in as excess or unserviceable, and disposal operations).

(a) In the acquisition management phase of LOGSEC, CID elements apply investigative effort to support requiring activities and acquisition program managers through each phase of the systems acquisition lifecycle model, including concept exploration, research and development, system development and demonstration, production and deployment, and operations and support. This area of LOGSEC operations will routinely be performed by Major Procurement Fraud Unit (MPFU) elements, usually in CONUS locations.

(b) The distribution phase of LOGSEC operations is the most fluid phase in the LOGSEC mission, and it can present the greatest vulnerability to Army materiel. This phase includes the functions of land, rail, air and sea transportation, as well as storage and warehousing of materiel before release to intermediate supply activities or deployed units. Vulnerabilities to materiel are most prevalent at nodes in the LOGSEC pipeline where changes in the mode of transportation occur. In the distribution phase of LOGSEC operations, CID elements enhance security of shipments in transportation channels in CONUS and OCONUS locations. In part, this is accomplished through effective liaison with the U.S. Army Military Traffic Management Command (MTMC), the U.S. Transportation Command (USTRANSCOM), and through proactive investigative efforts by CID elements worldwide. Ensuring effective CID support is provided to MTMC and USTRANSCOM is the responsibility of the Director, MPFU, who will assign a liaison officer to the Operations Center, MTMC to act as the CID representative to that command. This liaison officer will serve as the CID conduit to receive MTMC requests for vulnerability assessments of strategic ports, to identify conditions or situations requiring CID interest, and to report criminal activity affecting MTMC operations. Routine information exchange between the CID MTMC liaison officer, the various field CID field elements and the Economic Crime and LOGSEC Branch, DCSOPS, HQUSACIDC, is essential in supporting the command’s overall LOGSEC mission. There will be no hindrance to the exchange of information between CID elements or levels of command. Criminal investigative efforts in the distribution phase of LOGSEC operations will routinely be performed by all CID elements as military assets move through the logistics pipeline.

(c) Proactive investigative efforts performed in the distribution phase of LOGSEC operations include, but are not limited to, LOGSEC awareness briefings provided to deploying commanders, criminal activity threat assessments of areas along transportation routes, crime prevention initiatives at ports of debarkation and embarkation, briefing and debriefing super cargo personnel, reviewing causes of frustrated cargo, performing physical security examinations of railheads, ports, staging areas, and warehouses, and reviewing contingency contracts and Logistics Civil Augmentation Program (LOGCAP) contracts in forward deployed areas for indications of fraud, theft and other criminal acts. Proactive efforts in the distribution phase of LOGSEC operations are performed by all elements of CID in all CONUS and OCONUS locations.

(d) The materiel management phase of LOGSEC operations focuses on the security of materiel after it has been delivered by the transportation providers to the intermediate supply activities. At an installation, investigative support is provided to Accountable Officers at Supply Support Activities (SSA), Materiel Management Centers (MMC), and the Army Materiel Command (AMC) Single Stock Fund Manager. In forward deployed areas of operation, this support will be provided to forward supply bases where materiel is stored or warehoused before issue to the customer. In this phase of LOGSEC operations, attention may be applied to reviewing the legitimacy of requisitions and maintenance service orders, receipt and issue procedures, accountability procedures, identification and recovery of diverted materiel, and accountability of retrograde materiel. This phase of LOGSEC operations will normally be performed by military CID elements at posts, camps, stations and in forward deployed areas of operations.

(5) LOGSEC operations in forward deployed locations occur in a joint service environment. Geographic theater commanders may deploy elements of each service component to support peacekeeping, contingency or war operations as required. For this reason, the first step in any forward deployed LOGSEC operation must be to perform an effective mission analysis. The analysis must consider the investigative assets of the US Navy and the US Air Force Office, especially at sea, rail and aerial ports of embarkation in the theater of operation, as well as host country military or police authorities present. The mission analysis should identify the responsibilities and capabilities of each agency, and the actual logistics pipeline depicting key routes of travel and nodes where the mode of transportation may change. These seams in responsibilities and in the flow of materiel are often the areas of greatest vulnerability, and may indicate the location where deployment of CID investigative assets may be appropriate. The Economic Crimes and LOGSEC Branch, DCSOPS, HQUSACIDC, in conjunction with the various Group Operations personnel, will provide assistance, as required, to subordinate commands in performing the LOGSEC mission analysis.

(6) The capabilities of CID’s LOGSEC efforts are best realized through the integration of its many components working in concert with each other under an overarching management that ensures a coordinated focus. The EC and LOGSEC Branch at HQUSACIDC will support and coordinate USACIDC LOGSEC operations globally. In times of increased global conflict, and as directed by the CG, USACIDC, the mission of the Branch will intensify to support overall Army and DoD needs. To staff the Branch during increased operations, the DCSOPS is authorized to request mobilization of Reserve or National Guard CID personnel or to task the major subordinate commands to provide personnel and expertise to meet mission needs.

10-2
DoD policies concerning economic crime investigations

a. The DoD Instruction 5505.2, Subject: Criminal Investigations of Fraud Offenses, provides that the DoD Inspector General (DoDIG) has the responsibility to conduct, supervise, monitor, and initiate investigations relating to fraud within the DoD and those other investigations deemed appropriate by the DoDIG. The instruction establishes policies, responsibilities, and procedure for determining which of the DoD criminal investigative organizations (DCIO) will conduct investigations of fraud offenses under the U.S. Code and Uniform Code of Military Justice.

b. The DoD Directive 7050.5, Subject: Coordination of Remedies for Fraud and Corruption Related to Procurement Activities, provides policy, procedures, and responsibilities for the coordination of criminal, administrative, and contractual remedies stemming from investigation of fraud or corruption related to procurement activities. The directive emphasizes that more effective and timely communication of information developed during such investigations will enable the DoD to take the most appropriate of the available measures.

10-3
Jurisdiction

Fraud investigations within the Department of Army are undertaken for the primary purpose of furthering a function of the DoD (See DoD Instruction 5505.2, paragraph D.4). The jurisdiction of such investigations extends to all persons and organizations affiliated with the DoD. As such, the restrictions of the Posse Comitatus Act (18 USC 1385) are not applicable. Additionally, the Posse Comitatus Act does not apply to investigations conducted by, or under the direction of, or at the request of the DoDIG, (5 USCA appendix 3, section 8(g)).

10-4
Economic crime offenses

These offenses assimilate all of the traditional concepts connected with fraud and deceit.

a. Elements of economic crime offenses. Although a universal definition of economic crime does not exist, most authorities accept five common elements as being present in an economic crime offense.

(1) Intent (mens rea) to commit a wrongful act or to achieve a purpose inconsistent with law or public policy.

(2) Disguise of purpose or intent, wherein the offender tries to make the act appear legitimate. Once the crime is detected, it may tend to prove the element of intent.

(3) Reliance on ignorance or carelessness on the part of the victim. The sheer size and volume of business conducted by the Army normally provides this element.

(4) Acquiescence by the victim, whereby the offender induces the victim to undertake an act, either inadvertently or voluntarily, through the employment of disguise.

(5) Concealment of the crime.

b. Some of the types of criminal acts that comprise the generic term "economic crime" are:

(1) Violation of public trust. These offenses include bribery, graft, conflict of interest, soliciting and/or receiving gratuities, unauthorized employment, and violations of the Trade Secrets Act.

(2) Fraud/false statements. This includes making false official statements, altering documents, forgery, false certifications, false vouchers, and perjury.

(3) Contract fraud/false claims. This includes making or presenting false claims, contracting or the obligation of funds in excess of appropriations, insufficient delivery of products or services, product substitution and illegal kick backs.

(4) Miscellaneous. Obstruction of justice, racketeering and corrupt practices (i.e., RICO) and violations of the Sherman Anti-Trust Act are examples of miscellaneous offenses.

10-5
Economic crime investigative responsibilities

The provisions of DoD Instruction 5505.2, Criminal Investigation of Fraud Offenses, determine the specific responsibility for the investigation of fraud offenses within the DoD. The four defense criminal investigation organizations (DCIO): USACIDC, U.S. Air Force Office of Special Investigations (OSI), Naval Criminal Investigative Service (NCIS), and the Defense Criminal Investigative Service (DCIS); share responsibility for the investigation of fraud offenses affecting the DoD. USACIDC's investigative responsibilities for the investigation of fraud offenses are further clarified below:

a. DoD activities. DCIS has the investigative responsibility for all DoD activities to include, Office of the Secretary of Defense (OSD), Joint Chiefs of Staff (JCS), and the Strategic Defense Initiative Organization (SDIO) with the following exceptions:

(1) When the DoDIG or his/her designated representative deems it appropriate to refer the investigation to USACIDC.

(2) When allegations of fraud involving a SDIO are received by or arise during an ongoing USACIDC investigation, the investigating USACIDC element will coordinate the information with the DCIS and, absent any unusual circumstances, will conduct a joint investigation.

(3) When the investigation involves the DoD Education Activity (DoDEA) supported by an Army activity or installation, the investigative responsibility belongs to the USACIDC.

b. The Defense Logistics Agency (DLA):

(1) Allegations of contract fraud regarding contracts awarded and administered by the DLA are the investigative responsibility of the DCIS. See paragraph e below.

(2) The Defense Reutilization and Marketing Services (DRMS). DCIS has investigative responsibility for DRMS offices except the following:

(a) The USACIDC has investigative responsibility for fraud investigations involving DRMS when the DRMS office or off site branch office is located on an Army installation.

(b) The DoDIG may designate DRMS offices, not located on a military installation to be USACIDC's investigative responsibility.

(3) The Defense Fuel Supply System (DFSS). DFSS in the European and Pacific theaters are administered by DLA and are the investigative responsibility of DCIS. Any allegations involving the DFSS that are developed or received by USACIDC during the conduct of other investigative activity will be promptly reported to the nearest DCIS field office.

c. Unified/Specified Commands. USACIDC has the investigative responsibility for investigations involving unified/specified commands when they are hosted/supported by an Army installation/activity.

d. Special Operations Forces Low Intensity Conflict (SOFLIC) units. The USACIDC has investigative responsibility for investigations of Army components

of SOFLIC units. All allegations of fraud involving a SOFLIC unit will be reported to HQUSACIDC, ATTN: CIOP-CO. HQUSACIDC will be responsible for notifying HQs, DCIS of all such USACIDC investigations. This does not preclude routine exchange of information between USACIDC and DCIS field elements, and it does not preclude the initiation of a joint investigation into such allegations.

e. Allegations of fraud on contracts awarded by the Army.

(1) Allegations of fraud on contracts awarded and administered by the Army are the investigative responsibility of the USACIDC.

(2) Contracts awarded by the Army and administered by DLA through the Defense Contract Management Command (DCMC) are the joint responsibility of DCIS and USACIDC.

f. USACE military construction or civil works projects. Fraud or theft allegations involving USACE military construction or civil works projects are the joint responsibility of DCIS and USACIDC when:

(1) The potential loss is $100,000 or more; or,

(2) The subject of the investigation is a district engineer, resident officer in charge, a public works officer, a retired military officer in the grade of O-6 and above, or a civilian employee in the grade of GS/GM-15 or above and the potential loss to the U.S. Government is $5,000 or above; or

(3) Any criminal corruption allegation related to procurement involving current or retired DoD military or civilian personnel; or

(4) Any investigation into defective products or product substitution in which a serious hazard to health, safety, or operational readiness is indicated, regardless of the value of the loss; or

(5) Any allegation of criminal activity which has received or is expected to receive, or if disclosed, could be expected to receive significant media coverage.

(6) All other allegations of fraud and other criminal activity that involves USACE components are the investigative responsibility of the USACIDC. Based upon the criteria in paragraph 4-12, this regulation, and in accordance with these instructions, a joint investigation should be conducted in order to ensure that HQUSACIDC and the Army remains apprised of fraud or theft allegations concerning USACE activities.

g. The North Atlantic Treaty Organization (NATO). Allegations of fraud relating to NATO are the investigative responsibility of the DCIS. When an allegation(s)

relating to NATO projects involve Army installations a joint investigation by USACIDC and DCIS should be conducted.

h. Violations of the Antikickback Enforcement Act of 1986 which are voluntarily disclosed by a contractor are the responsibility of the DCIS except as follows:

(1) If the contract is awarded or administered by the Army, or the Army is involved in the performance of the contract, a joint investigation should be conducted.

(2) Allegations of fraud and violations of the Antikickback Enforcement Act of 1986 which are developed during the conduct of routine investigative activity and were not voluntarily disclosed by a contractor, are the investigative responsibility of USACIDC. USACIDC components that initiate ROIs that involve alleged violations of the Antikickback Enforcement Act that meet the criteria of paragraph (1) above, shall promptly coordinate with the nearest DCIS field office.

10-6
USACIDC management responsibilities

a. The Office of the DCSOPS, HQUSACIDC will:

(1) Oversee, coordinate and provide guidance for economic crime investigations and LOGSEC efforts of CID to ensure there is cohesive and effective coverage as well as crime prevention effort applied in all environments, from peace through war.

(2) Resolve disputes involving investigative responsibility and jurisdiction between CID activities that cannot be resolved between the concerned USACIDC major subordinate commands.

(3) Update the command economic crime and LOGSEC policy and doctrine based on operational variables and recommendations from subordinate command and HQUSACIDC staff elements.

(4) Assist field elements by providing or obtaining technical assistance for complex investigations.

(5) Coordinate training opportunities to improve the effectiveness of the economic crime and LOGSEC missions to include:

(a) Support the USAMPS Advanced Fraud Training Course

(b) Provide mobile training sessions to active, reserve and National Guard USACIDC elements.

(c) Support fraud training to supporting agencies.

(d) Arrange ad hoc training sessions related to economic crimes and LOGSEC.

(e) Convene EC/LOGSEC workshops as needed to evaluate and target economic crime threats to the Army.

(6) Receive, process and monitor DoD Hotline allegations referred by the DoD or the Department of the Army IG.

(7) Ensure coordination with OTJAG all investigations involving allegations of procurement fraud in accordance with AR 27-40.

(8) Monitor the selected EC and LOGSEC investigations, operations and crime prevention surveys.

(9) Coordinate with DoD/DA staff elements and major Army commands concerning requests for economic crime investigative, LOGSEC or CPS support.

(10) Establish command wide priorities in LOGSEC Operations.

(11) LOGSEC intelligence and information from all sources (internal and external) and ensure timely dissemination to subordinate elements.

(12) Support subordinate elements by performing top-level mission analysis of contingency operations, deployments and war to identify key nodes and ports of debarkation and embarkation; assist CID Groups in identifying LOGSEC team requirements and locations; provide guidance and oversight of LOGSEC missions.

(13) Exercise quality control and technical review of completed EC, LOGSEC and CPS reports.

(14) Serve as a conduit to ensure information is readily exchanged between the various CID elements of the entire command.

b. The Office of the DCSSPT, HQUSACIDC, will:

(1) Coordinate with Civilian Personnel Offices about vacancy announcements for civilian criminal investigators for the economic crime program.

(2) Budget for economic crime training requirements.

(3) Ensure there are sufficient numbers of economic crime trained CID agents assigned throughout the command to meet contingency operations.

c. The USACIDC major subordinate commands will:

(1) Appoint an accredited CID Special Agent to coordinate and oversee economic crimes investigations and LOGSEC operations within the subordinate command's area of responsibility (or functional area of responsibility for the 701st MP Gp).

(2) Coordinate with DCSSPT for the assignment of a sufficient number of economic crime trained agents to combat the economic crime and LOGSEC threat within their area of operations.

(3) In conjunction with DCSOPS, perform mission analysis for each LOGSEC operation in AOR.

(4) Provide timely reports of LOGSEC intelligence and information to HQUSACIDC DCSOPS.

(5) Perform LNO functions at key logistics providers as directed by CIDR 195-1, Appendix E, and ensure information is disseminated throughout CID.

(6) Provide LOGSEC trained personnel to support missions in AOR.

(7) Support Army Commanders through effective coordination, oversight and guidance for LOGSEC operations in each respective AOR.

(8) Submit requests for changes of economic crime positions to HQUSACIDC.

(9) Ensure that only a qualified senior economic crime supervisor (ASI 9E) special agent functions as the USACIDC major subordinate command economic crime staff officer. A senior military agent who does not possess ASI 9E may be utilized as an economic crime staff officer, providing that the individual is programmed for mission related training as prescribed in paragraph 10-44.

d. Battalion/district/field office commanders:

(1) Appoint an accredited CID special agent officer to coordinate and oversee economic crimes investigations and LOGSEC operations in peace and war in the respective geographical area.

(2) Perform mission analysis for LOGSEC operations in the respective geographical area.

(3) Manage, supervise and perform LOGSEC operations in support of the Army commanders.

(4) Provide timely reports of LOGSEC intelligence and information to Group Economic Crime Staff Officer (ECSO) / LOGSEC Officer.

10-7
Economic crime investigative procedures

a. The USACIDC retains the responsibility to investigate those contract fraud matters wherein the U.S. Army is involved in the contracting process, including award, administration and/or performance or in which there is an Army interest. This responsibility may, however, be exercised jointly with other DCIOs in accordance with DoD Instruction 5505.2. USACIDC will conduct a joint investigation with another DCIO:

(1) Whenever there is a significant investigation in which the concerned contract involves issues that impact on the Army's logistics system, the Army's ability to maintain combat readiness, and/or safety issues.

(2) Whenever the DCIS or military criminal investigative organization (MCIO) initiates an investigation in which there is an Army interest, complete participation in joint investigations is not required; rather resources that can be made available by the USACIDC unit will be committed to support the investigative effort. The USACIDC should normally participate in joint investigations. Except for initial notification, DCIS does not normally furnish information concerning ongoing investigations in which there is an Army interest to USACIDC elements unless USACIDC participates in the investigation.

(3) An incident involving the DLA or USACE in which there is an Army interest will be reported by the affected DLA or USACE district office directly to the concerned USACIDC and DCIS office. The USACIDC component receiving such notification will immediately coordinate with the nearest DCIS field office. Whenever a USACIDC component uncovers an allegation of fraud that meets the joint investigative responsibility criteria outlined in paragraph 10-5 above during the conduct of other investigative activity, it will immediately coordinate with the concerned DCIS field office.

(4) Whenever the U.S. Army is affected by fraud, the USACIDC will be involved in the investigation, regardless of other agency jurisdiction. This will be accomplished by:

(a) Monitorship by HQUSACIDC of the investigation of other DoD and federal agencies. Field elements may be tasked to assist in this effort.

(b) The conduct of joint investigations with other DCIOs or federal agencies whenever possible.

(c) Based upon the criteria in paragraph 4-12, this regulation, and in accordance with these instructions, a joint investigation should be conducted in order to ensure that HQUSACIDC and the Army remains apprised of fraud allegations concerning contracts in which there is an Army interest.

(d) Except as specified, fraud investigations in which there is an Army interest will not normally be referred to another federal or DoD investigative agency for investigation.

(e) Declinations to participate in a joint investigation within the criteria established by paragraphs 10-5e(2) and 10-5f will only be made with the concurrence of HQUSACIDC, ATTN: CIOP-COP-CO. Other than this, USACIDC components may elect to initiate either a referred or collateral ROI in accordance with paragraphs 7-20 and 7-21 of this regulation.

(5) If the DCIS or MCIO declines to undertake a joint investigation and the USACIDC activity believes such is necessary to represent Army interests adequately, the matter should be referred to the concerned USACIDC major subordinate commander or HQUSACIDC, ATTN: CIOP-CO, as appropriate for resolution with the headquarters of the other investigative organization.

b. Notification of allegations of suspected fraud that result from the DoD Voluntary Disclosure Program (see paragraph 10-8) will be made by the Assistant Inspector General, Criminal Investigative Policy and Oversight (CIPO), DoDIG to HQUSACIDC and DCIS.

c. Defense Contract Audit Agency (DCAA) early alert notices (DCAA Form 2000) will be forwarded by DCAA to the CIPO. The CIPO will, upon receipt of the DCAA Form 2000, make further notification to HQUSACIDC and DCIS.

d. The USACIDC shall promptly notify the originating DCIS organization whenever:

(1) A matter referred for investigation is declined; or

(2) Whenever USACIDC for any reason terminates an investigation initiated by the DCIS, prior to completion.

(3) The USACIDC shall provide the DCIS a copy of the complete ROI which was initiated as a result of the DCIS referral.

e. The USACIDC shall expeditiously inform the other DCIOs whenever a matter under investigation affects an activity under the jurisdiction of or assigned by

DoDI 5505.2 to another DCIO. Whenever the interests of any DoD component otherwise warrant such notification:

(1) The USACIDC will provide detailed information on the allegation to the affected DCIO, and upon completion of the investigation a copy of the completed ROI.

(2) If either the AFOSI or the NCIS refers an investigative matter to the USACIDC and an investigation is not initiated, or if such an investigation is terminated prior to completion, that agency will be promptly notified. Copies of completed reports of investigation for such referrals will be provided to the referring DCIO.

f. The USACIDC will provide notice of all investigations that involves a function or service provided by the DLA. Such notification will be made as soon as the DLA interest is determined, and in such a manner so as not to compromise the investigation. Notification will be made to:

(1) The nearest DCIS field office.

(2) The DLA fraud counsel for the concerned activity.

(3) The Staff Director, Office of Command Security, DLA Headquarters (ATTN: DLA-I).

(4) During the conduct of these investigations, distribution of status reports and completed reports of investigation will be made in accordance with this regulation and will also be provided to the DCIS and the Staff Director, Office of Command Security, DLA Headquarters (ATTN: DLA-I).

g. Significant allegations of bribery and conflict of interest as specified in paragraph 4-14 a(1) of this regulation will be referred to the FBI.

(1) Other than as noted in this regulation significant allegations of fraud within the DoD (except those cases in which there is an Army interest) will be referred to the DCIS before being referred to any investigative agency outside DoD.

(2) The USACIDC will investigate all matters in which there is an Army interest referred to it by the DCIS.

h. In the event the DCIS declines to investigate any matter referred to it by the USACIDC, one of the following will be accomplished:

(1) The USACIDC will conduct the investigation, if there is an Army interest.

(2) The matter may be referred to other appropriate agencies for investigation, to include the military police.

(3) The matter may be prioritized for future investigation, if there is an Army interest.

(4) If no investigation is undertaken by any agency, and the information or allegation was reported to the USACIDC by an outside organization or activity, the USACIDC element receiving the complaint will inform that organization or activity of the status of the matter and why no investigation is being undertaken.

i. Under the provisions of DoD Instruction 5505.2, USACIDC is required to notify DCIS of any allegation of fraud involving certain DoD or Army organizations.

j. HQUSACIDC will be notified by Initial/SSI, ACIRS electronic mail, or by electrical message of the initiation of any investigation of fraud involving the following:

(1) The Strategic Defense Initiative Organization (SDIO).

(2) Special Operations Forces - Low Intensity Conflicts (SOFLIC).

(3) The U.S. Army Corps of Engineers (USACE). In addition to normal SSI criteria, USACIDC field elements will notify HQUSACIDC of any investigation involving the USACE as specified in paragraph 10-5f.

10-8
Criminal Investigation of Fraud Offenses

a. General. The USACIDC is committed to working together in a spirit of cooperation with the NCIS, AFOSI and the DCIS while at the same time ensuring the USACIDC remains responsive to the needs of the Secretary of the Army and Army commanders.

b. Policy. In determining investigative jurisdiction, the intent is to reduce to the extent possible the number of joint investigations. Joint investigations will be considered only when one or more of the factors specified in this section are present. There is no requirement to notify the DCIS or conduct a joint investigation with the DCIS simply because an Army contract is being administered by the Defense Logistics Agency (DLA). The same holds true for fraud involving U.S. Army Corps of Engineer construction, civil works or environmental cleanup contracts. Basic jurisdictional responsibilities between the three military criminal investigative organizations (MCIO) and the DCIS are as follows:

(1) The military criminal investigative organizations are responsible for the following:

(a) With the exception of those cases specified below, all contracts and procurement actions awarded by a military department, regardless of what organization administers the contract.

(b) Allegations of fraud involving the Defense Finance and Accounting Service (DFAS) to the extent the allegations pertain to the DFAS providing services for a single post, camp, base, facility or installation level activity of a military department, or pay and allowance or travel fraud by a civilian employee or service member in a military department.

(c) Activities of the Defense Reutilization and Marketing Service (DRMS) and Defense depots outside the Continental United States (OCONUS). Additionally, any allegations resulting from a compromise of physical security of the DRMS, depot, or the host installation (e.g., break-ins, theft of property), subject to normal USACIDC jurisdictional thresholds specified in AR 195-2.

(d) The activities of or at an individual installation or facility, especially those over which the installation commander has contracting authority or that effect the health, welfare and morale of military service personnel (or their dependents) assigned to that specific installation of facility, including circumstances where the allegations pertain to the activities of or at a military installation or facility supported by another installation or facility. It also includes Department of Defense dependent schools both within CONUS and OCONUS.

(e) All matters regarding the Army and Air Force Exchange Service, the Navy Exchange Services Command, the Marine Corps Exchange at any level and all nonappropriated fund activities.

(f) Allegations of fraud perpetrated against OCHAMPUS, a fiscal intermediary or other health care providers or insurers by military service members, military retirees and dependents who have received, made claims for or requested benefits or services under such programs or operations.

(g) Construction contracts funded solely by one military department.

(h) All Unified Combatant Commands including special operations forces low intensity conflict organizations (SOFLIC).

(i) All Defense Fuel Supply Agency activities in the European or Pacific Commands.

(j) All NATO projects and expenditures by the DoD in connection with NATO projects or activities.

(k) Except as provided by this section, allegations of bribery of a military service member or civilian employee of a military department.

(2) The Defense Criminal Investigative Service is responsible for the following:

(a) The Office of the Secretary of Defense (OSD) and its field activities.

(b) The Joint Chiefs of Staff (JCS).

(c) All contract and procurement actions awarded by the Defense agencies, their components and field activities, with the exception of those specified above.

(d) All DRMS and Defense Distribution Depot activities, with the exception of those specified above. The DCIS shall, except under exigent circumstances or for reasons of operational security, first notify the cognizant MCIO office within 72 hours of the initiation of all investigations conduced under this provision regarding a DRMS or Defense Depot activity on such installation. Any notice to or briefing of the installation commander shall then only be accomplished by the DCIS with the participation of the cognizant MCIO.

(e) Allegations of fraud committed by health care providers, to include “partnership agreement” situations, under the OCHAMPUS program and fiscal intermediaries thereto.

(f) Allegations of suspected violations of the Antikickback Enforcement Act of 1986 that are required to be reported by contractors under the statute whether or not reported by such contractors.

(g) All kickbacks or bribery involving civilian employees of the OSD, JCS, and the Defense agencies and their field activities.

(h) Any allegations that the IG, DoD, pursuant to the Inspector General Act of 1978, as amended, considers appropriate for investigation by the DCIS.

(3) Investigative jurisdiction is shared between the DCIS and MCIOs in those cases where allegations of fraud involve a contractor (to include employees, officers, divisions, subsidiaries both wholly or partially owned or controlled, and subcontractors where the subcontractor is an affiliated or owned entity) that has contracts with more than one DoD component and in cases of antitrust violations. In all of these cases, investigative responsibility and whether an investigation is to be conducted jointly will be determined by the appropriate jurisdictional responsibility working group established below. It is USACIDC policy that in all cases of an Army awarded and funded contract, primary investigative jurisdiction and responsibility rests with the USACIDC with there being no need for a joint

investigation unless clearly appropriate under the factors listed within this section and agreed to by the appropriate jurisdictional responsibility working group.

(4) Major subordinate commanders will provide representation to appropriate jurisdictional responsibility working groups established in coordination with the other MCIOs and the DCIS. Representatives to these groups will be battalion commanders or special agents-in-charge of resident agencies or fraud field offices. These representatives will be authorized to agree to assignment of investigative responsibility for allegations being considered by the group.

(5) All allegations of fraud of the type included above or other allegations involving jurisdictional issues not resolvable under this interim guidance will be referred within 72 hours of receipt to the USACIDC representative of the appropriate jurisdictional responsibility working group for resolution. The USACIDC representative will bring the allegations to the attention of the working group in accordance with local procedures for a jurisdictional decision. Pending this decision, the investigative unit receiving the allegation will not open any preliminary investigation or make any presentation to prosecutive authorities. Sequence numbers will, however, be assigned in accordance with existing procedures. Prosecutors or staff judge advocates may be contacted in exigent circumstances, however, the circumstances will be documented and provided to the USACIDC representative on the appropriate jurisdictional responsibility working group.

(6) Whether a joint investigation is appropriate will be determined by the jurisdictional responsibility working group using the following criteria:

(a) The alleged fraud involves and impacts substantially on the funding, programs, property or personnel (as subjects) of more than one DoD component.

(b) The nature of the investigation requires the commitment of more resources than a single MCIO or the DCIS can reasonably provide.

(c) Participation by more than one investigative agency (MCIO/DCIS) is required by some other DoD level policy or memorandum of understanding applicable to the circumstances of the case.

(d) The matter being investigated is considered to be of such importance to a military department that participation by more than one investigative agency (MCIO/DCIS) may avoid any appearance of lack of independence or possible command influence. Within the USACIDC, this determination will be made by the appropriate major subordinate commander. The Commander, 701st MP Gp (CID), may delegate this authority to the Director, MPFU.

(e) The IG, DoD, may determine that any investigation will be conducted jointly or that the DCIS will be a joint participant in any joint investigation by any other MCIO.

(7) When a determination is made that a joint investigation is appropriate, the guidelines below are applicable. When it is determined that a joint investigation is not appropriate, the guidelines in paragraph b below will be used in designating the investigating agency:

(a) Substantive activity. Investigating agencies (MCIOs/DCIS) participating in the joint investigation will supply personnel to perform substantive and regular investigative activities in furtherance of the investigation.

(b) Lead agency. The lead agency will be determined by the following criteria (these elements are also used by the investigative responsibility working groups to determine which agency has jurisdiction in non-joint cases:

1. Mutual agreement of the members of the investigative responsibility working group.

2. The organization that developed the information giving rise to the investigation in proactive cases.

3. The organization with the greatest amount of available resources experienced in the type of fraud being investigated.

4. The extent of the IG, DoD, interest in the matter pursuant to the statutory mandates of the IG, DoD, or congressional or DoD management interest. This implies that there has been an affirmative statement of such interest by the IG, DoD.

5. The organization representing the military department with the greatest potential loss or harm and the extent of the interest of the Secretary of the Military Department.

6. The expressed interest, if any, of the government or military authority responsible for the prosecution or civil litigation for the investigation in question.

(c) Lead agency responsibilities. The lead agency will be responsible for:

1. Notifying the centralized points of coordination for the affected DoD components and ensuring the centralized point of coordination is provided, on a timely basis, any and all information needed to implement, update, or revise the remedies plan.

2. Originating and processing all requests for electronic surveillance, search warrants and similar investigative techniques requiring approval outside the MCIO or DCIS.

3. Establishing the format for preparation of all reports of investigation, memoranda for record, memoranda of interview, witness statements and other related documentation.

4. Reporting all investigative outcomes for inclusion in the IG, DoD, Semiannual Report to the Congress in a timely and accurate fashion and any other required reporting (e.g., under National or Defense Incident Based Reporting Systems).

5. Making all formal and informal presentation of the case for prosecutive (civil or criminal) determinations. Representatives of other participating MCIOs or the DCIS may accompany the lead agency when it would result in a more effective or complete presentation of the case.

6. Preparing and submitting any referrals to the IG, DoD, for application of the Program Fraud Civil Remedies Act.

(8) The following actions will be taken for every fraud investigation, meeting the requirements set forth in this section, referred to a field working group for a jurisdictional determination:

(a) If the USACIDC is identified as having sole jurisdiction for an investigation or is determined to be the lead agency in a joint investigation, the USACIDC unit will complete the appropriate documentation and forward (FAX) it to the DoDIG.

(b) A statement will be included in the summary portion of all initial reports of investigation sent to the DoDIG per this section, summarizing the results of the working group meeting, to include the DCIOs involved in the investigations, which DCIO is designated as lead agency and the reasons for the decision.

(c) If, for any investigation originating as a joint investigation, one or more DCIO declines further investigative involvement, a copy of the status report reflecting this fact will be sent to the DoDIG.

(d) For all joint investigations, a copy of the first page only of the final report of investigation, will be forwarded to the DoDIG.

(e) The worksheet and any status or partial final reports of investigation will be forwarded to the DoDIG, ATTN: CIPO, 400 Army Navy Drive, Suite 725, Arlington, VA 22202-2884, Fax (703) 604-8720.

(9) Questions about or conflicts arising from the interpretation of the DoDIG interim guidance will be first addressed by the appropriate jurisdictional responsibility working groups. Any unresolved issues will be referred through major subordinate commanders to HQUSACIDC, ATTN: CIOP-ZA. Efforts will then be made to resolve the issues with the appropriate MCIO or DCIS headquarters. If this is not possible, the matter will be referred to the Inspector General, Department of Defense, for final arbitration.

(10) All CID field units will forward a copy of each Initial/SSI report concerning the initiation of a fraud investigation to the Inspector General, Department of Defense. Instructions for addressing the DoDIG through the ACIRS system:

(a) The message address for the DoDIG will be included in the next change package for ACIRS in the “Non-CID” “CONUS” address table.

(b) Until this change is installed, the following procedures can be followed to add the DoDIG to local plain language address (PLA) tables:

1. When creating an ACIRS message, select “Local” from the Addressees menu.

2. Select “Add” from the Local Address Administration menu. An input window will be displayed.

3. In the display window enter:

PLA OFC OF DODIG WASH DC
E-Mail general%po%cipo@dodig.osd.mil
Office CIPO

4. Once the address has been entered, it may be selected from the “Local” PLA table for future messages.

5. All Initial/SSI ROIs involving the following Inspector General Report Codes (Alpha-Numeric) require distribution directly to the DoDIG (Forwarding of Status and Final ROI not required):

IG Code	Offense
A	Bribery/Solicitation of Bribe (Government Official)
B	Conflict of Interest
C	Pay and Allowance Fraud
D	Antitrust Act Violation
E	Procurement Fraud

F	Redistribution and Marketing Fraud
G	Commissary/Subsistence Activity Fraud
H	Nonappropriated Funds Fraud
I	CHAMPUS Fraud
J	Government Theft/Larceny/Embezzlement ($100,000 and above)
L	Personnel Action Frauds
M	Government Theft/Larceny - Combat Vehicles, Weapons, Explosives and Munitions ($100,000 and above)
N	Gratuities (Government Officials)
P	Program Management Irregularities
S	Environmental Crimes

(11) In cases of larceny of government property, the Initial/SSI reports will be forwarded only if the known or suspected loss to the government exceeds $100,000. Copies of Initial/SSI reports will also be forwarded for the following:

(a) Those offenses listed in chapter 7 of this regulation.

(b) Any criminal corruption case relating to procurement that involves active or retired DoD personnel.

(c) Any criminal case, regardless of the allegation, that has received, is expected to receive, or that if disclosed could reasonably be expected to receive significant media coverage.

(d) In preparing these Initial/SSIs, drafters will ensure that the subject of the investigation is identified together with the identification of any other investigative organization, their ROI number in the case of joint investigations, the source of the allegation(s), and the predication for opening the case. There is no requirement to send status reports to the DoDIG.

(12) Allegations of fraud involving any program, operations, or personnel of the DoD will not be referred to any investigative organization outside the DoD without prior notice to HQUSACIDC unless the referral is required by DoD Directive 5525.7, Implementation of the Memorandum of Understanding Between the Department of Justice and Department of Defense Relating to the Investigation and Prosecution of Certain Crimes (see paragraph 4-14) or is otherwise specifically required by statute or regulation. Consultations with civilian law enforcement agencies to determine if a joint investigation is to be conducted on matters of mutual interest are not considered a referral.

10-9
Voluntary Disclosure Program

a. The DoD has established a formalized program encouraging DoD contractors to disclose voluntarily problems affecting their corporate contractual relationships with the DoD. Such disclosures are made by contractors without advance agreement regarding possible DoD resolution of the matter. The purpose of the program is to encourage DoD contractors in the voluntary policing of their internal operations and the reporting to appropriate DoD agencies of problems identified through such self-policing efforts. This allows the DoD to recoup losses of which it might not otherwise be aware, and supplements the detection assets available to the DoD.

b. Under this program, matters not involving potential criminal issues are to be presented to the appropriate contracting officer or DCAA auditor. Any issues involving criminal or civil fraud issues are to be reported to the DoDIG.

c. The determination of whether a particular disclosure will qualify as a voluntary disclosure is made by the DoDIG. Although this determination will normally be accepted by the Department of Justice (DOJ), DOJ reserves the right to make their own determination of voluntariness for purposes of prosecutive decision. Four specific criteria must be met if a contractor is to qualify as a "volunteer" under this program. These are:

(1) The disclosure by the contractor must not be triggered by the contractor's recognition that the underlying facts are about to be discovered by the U.S. Government through audit, investigation, contract administration efforts, or reported to the U.S. Government by a third party.

(2) The disclosure must be on behalf of the business entity, in contrast to admissions by individual officials or employees.

(3) There must be prompt and complete corrective action by the contractor, including disciplinary action and restitution to the U.S. Government where appropriate.

(4) After disclosure, the contractor must cooperate fully with the U.S. Government in any ensuing investigation or audit. "Cooperation" in any situation will depend upon the facts and circumstances of each individual case. The DoD may enter into a written agreement with a contractor making a voluntary disclosure which will describe the types of documents and evidence to be provided the DoD and resolve issues related to interviews, privileges, or other matters which may affect DoD ability to obtain all relevant facts in a timely manner.

d. Upon receipt of a voluntary disclosure, the DoDIG will schedule an initial meeting with representatives of the contractor, the appropriate suspension and debarment authority and the appropriate DCIO. T his meeting will allow early development of an understanding of the scope and the nature of the case, together with the investigative approach to be taken.

e. Voluntary disclosures which will require investigation by USACIDC will be forwarded to HQUSACIDC by the DoDIG. The DCSOPS, HQUSACIDC will, in turn, forward the matter by request for investigation to the appropriate USACIDC field element for investigation. The request for investigation will include any suggested investigative steps or investigative plan initially developed as a means of targeting the scope of the investigation.

f. All USACIDC field elements receiving requests for investigation involving voluntary disclosures by contractors will proceed with the investigation as expeditiously as possible. Copies of the initial and all status reports will be provided HQUSACIDC, ATTN: CIOP-COP-CO. The DCSOPS will forward copies of these reports, as it deems appropriate, to the Procurement Fraud Division (PFD), OTJAG.

g. The PFD will, based upon information provided by the investigating unit, make a determination whether the matter will be accepted for criminal prosecution or civil suit, referred to the appropriate U.S. attorney, or if prosecution/civil suit will be declined. If the matter is referred to a U.S. attorney, the investigating element will, from that point, coordinate the investigation with that U.S. attorney. If prosecution or civil suit is declined, a final report of investigation may be prepared. A copy of the final ROI will be provided by HQUSACIDC to the DoDIG for a determination of possible action under the Procurement Fraud Civil Remedies Act.

h. All USACIDC field elements receiving notices of referrals of voluntary disclosures from either contracting officers or U.S. Government contractors will immediately report such referrals to HQUSACIDC, ATTN: CIOP-COP-CO for coordination with the DoDIG.

i. Any circumstances which indicate that the contractor involved is not fully cooperating, is not complying with the terms of any agreement relative to full cooperation, or which may otherwise indicate that the contractor may no longer qualify for participation in the voluntary disclosure program will be reported immediately to HQUSACIDC, ATTN: CIOP-COP-PO for further referral to the DoDIG.

10-10
Coordination of investigations with the DPFU

This section is no longer applicable. Subsequent paragraphs will be re-numbered with version 5.0 of this regulation.

10-11
Program Fraud Civil Remedies Act

The Program Fraud Civil Remedies Act of 1986 (PFCRA) (Subtitle B, Title VI, P.L. 99-509; codified as 31 USC 3801 et. seq.) provides federal agencies with an administrative procedure for disposing of certain case s wherein false or fraudulent claims or false statements are submitted to the Federal Government. The act is applicable to false statements or claims or groups of related claims which total $150,000 or less if such statement or claim was made on or after 21 October 1986. It allows for the assessment of a civil fine of up to $5,000 for each such false claim or false statement. In addition, in lieu of damages, a person or business entity submitting a false claim may be liable for an assessment of up to twice the amount of any false claim which has been paid by the U.S. Government. The PFCRA should be considered as one more administrative remedy available to the Army, in addition to criminal prosecution, contractual remedies, civil litigation and other administrative remedies.

a. To establish a case under the PFCRA, it is necessary to establish, by a preponderance of evidence, that the maker or submitter of the claim or statement:

(1) Did so with actual knowledge that the claim was false or fraudulent; or

(2) Acted with "deliberate ignorance" of the truth or falsity of the claim or statement; or

(3) Caused submission of the claim or statement in reckless disregard of its truth or falsity; or

(4) Being under a duty to provide a material fact, omitted that fact, thereby, making the claim or statement false or fraudulent, and, in the case of a written statement, made an express written certification or affirmation of the truthfulness and accuracy of the statement. Proof of actual intent to defraud is not required.

b. Policy:

(1) The PFCRA will be considered for false claims and/or statements submitted by civilian personnel (including military family members) or business entities and former or retired military personnel.

(2) The PFCRA may be considered when military personnel have submitted false claims and/or statements and retired or otherwise left the military service prior to the time that any administrative or disciplinary action was taken.

(3) False statements/claims by active duty military personnel will be handled through normal military procedures; however, should a command decline to take action under the UCMJ, action under the PFCRA should be considered.

(4) Although legally permissible, the PFCRA will not normally be considered as an additional remedy against an individual or business entity which has been subjected to successful criminal prosecution. It may, however, be considered in conjunction with other civil or administrative remedies which may be available to the U.S. Government.

c. Procedures:

(1) Prior to recommending any case for action under the PFCRA, the investigating CID unit will coordinate with the appropriate procurement fraud advisor to ensure that action under the PFCRA is consistent with the total remedies package. The decision to refer a case for PFCRA consideration remains an investigative decision.

(2) If, after coordination with the procurement fraud advisor, the decision is made to proceed with PFCRA referral, a complete copy of the final ROI with all exhibits, supplemental reports, and relevant portions of the pertinent contract, if any, will be forwarded by memorandum of transmittal to the USACIDC major subordinate command staff judge advocate or MPFU operations division (ATTN: CISA-MOP) as appropriate. The memorandum of transmittal must include the name, address, and telephone number(s) of any DOJ personnel (Assistant U.S. attorney, PFD representative, etc.) who have been involved in the investigation. After review by the USACIDC major subordinate command staff judge advocate or MPFU operations division, all documentation will be forwarded to HQUSACIDC, CIJA-ZA as necessary, along with an endorsement.

(3) After reviewing the case and making a determination that PFCRA action may be appropriate, HQUSACIDC, CIJA-ZA or MPFU, will coordinate with the DoDIG and PFD to determine if any additional work needs to be done on the case. When acceptable, HQUSACIDC, CIJA-ZA or MPFU will forward the investigation to the DoDIG for their review as the statutory investigating official. The DoDIG will advise HQUSACIDC, CIJA-ZA or HQISA, whether the investigation will be referred to the Assistant Judge Advocate, General-Military Law (the designated Army reviewing official) for further proceedings.

(4) The investigating agents may be called upon to provide testimony and present evidence at hearings in the same manner as at criminal trials. Since the PFCRA is a civil proceeding, the respondent is entitled to discovery under rules which are broader than those in criminal trials. In this light, investigating agents may be subpoenaed to provide evidence and/or depositions to attorneys representing the respondent(s).

(5) The investigating CID unit must continue to track the case through the PFCRA proceedings for the purpose of determining the final disposition of the case. (It is anticipated that many cases may be settled through negotiations between the respondent(s) and the reviewing official prior to any formal hearing.) The results of action must be identified and reported in the same manner as in criminal actions.

10-12
Antikickback matters

Under the provisions of the Antikickback Enforcement Act of 1986 (Public Law 99-634, 41 USC 51-58) the DoDIG is authorized access to all facilities, books, electronic data and records of prime contractors of the DoD and their subcontractors for the purpose of determining compliance with the act.

a. All CID special agents have been designated by the DoDIG as official representatives for the purpose of such inspections conducted under the Antikickback Act. This authority applies only to enforcement measures for the Antikickback Act. No agreements between DoD contracting personnel and contractors should exist to limit the authority of the designated special agent or to determine or direct investigative techniques or operations. Special agents are cautioned not to enter into written or oral agreements with the contractor or subcontractor which in any way restricts access to facilities or records as described by the act without prior coordination and approval of HQUSACIDC.

b. This delegation of authority by DoDIG affords the special agent numerous advantages in antikickback investigations. It authorizes the special agent to enter a facility of a prime contractor of the subcontractor and access books, electronic data or other records without obtaining search warrants, DoDIG administrative or grand jury subpoenas, allowing the agent to pursue the investigation in an expedient manner. The act does not authorize the special agent to reproduce copies of extracts or seize evidence. Items that will be seized for evidentiary value must be obtained by means of a search warrant, DoDIG subpoena, or grand jury subpoena.

c. All CID special agents should make DoD contracting personnel within their assigned area of responsibility aware of this authority and request their

assistance in obtaining compliance with the provisions of the act. The DoD contractors should also be apprised of USACIDC's authority for access to all facilities, books, electronic data and records for the purpose of investigating suspected antikickback matters and that full assistance and cooperation should be provided to the special agent in gaining free access to such facilities and records. Additionally, when required for access, non-temporary government badges should be issued to the designated special agent(s) by the DoD contractor.

10-13
Screening of major contract accounting fraud cases

a. All USACIDC major contract accounting cases will be screened as directed below before any referral of the case is made to the criminal or civil divisions of the DOJ, or to a U.S. attorney's office (USAO) to:

(1) Ensure matters have been sufficiently and properly investigated.

(2) Identify accounting or contractual issues that may adversely impact on the successful civil or criminal prosecution of such cases.

(3) Expedite investigations and effectively use investigative resources on cases with significant fraud.

b. A major contract accounting fraud case includes any contract accounting fraud case, to include allegations of defective pricing and cost mischarging, where the dollar loss to the government is expected to exceed $500,000.

c. A referral to the DOJ or USAO shall include any of the following:

(1) A referral for a preliminary prosecutive opinion after some investigation has been completed.

(2) A referral for the commencement of a grand jury investigation or issuance of a grand jury subpoena.

(3) A referral for the purpose of seeking an application for a search warrant.

(4) Notification to a prosecutor of the existence of an investigation or a request for guidance at the initial stages of an investigation shall not be considered a referral for the purpose of DoDIG Memo 12, Subject: DoDIG Screening of Major Contract and Accounting Fraud Cases, 26 March 1990.

10-14
Screening and review procedures

a. Investigative screening and review

(1) Initial screening will be done by the originating CID element upon receipt of initial complaint/allegation or referral from the DCAA or other audit agency involving a major accounting fraud. Initial screening will be to determine if credible information exists to support the allegation and/or complaint. All subsequent investigation will be conducted until such time that a referral to the DOJ or USAO is considered appropriate.

(2) Prior to referral to the DOJ/USAO for appropriate prosecutive action the major contract accounting fraud investigation will be reviewed by a supervisory agent, providing that the supervisor has experience in working with major contract accounting fraud cases. If an experienced supervisor is not available, coordinate with the USACIDC major subordinate command for guidance.

(3) The review will be conducted to determine:

(a) If appropriate investigative steps are being accomplished.

(b) If adequate investigative and audit resources are available to support the investigation.

(c) If referral to the DOJ/USAO is appropriate.

b. Accounting/auditing review. The USACIDC supervisory investigator who is responsible for the investigative review, in coordination with the appropriate contract audit advisor, will:

(1) Ensure that adequate audit support is being provided to the investigation.

(2) Determine if there are any accounting issues that may adversely impact on the investigation.

(3) The contract audit advisor can be a qualified contract auditor who is:

(a) Assigned to USACIDC.

(b) A DCAA supervisory auditor.

(c) An Army Audit Agency supervisory auditor with contract audit experience.

(4) If a determination is made by the USACIDC supervisor and the contract audit advisor that further audit work must be accomplished before a referral can

be made, or that additional audit support is needed, they will coordinate with the responsible audit office to ensure that the required audit support is made available.

c. Legal review. The supervisory investigator will ensure that the case has been reviewed by an experienced procurement fraud attorney to determine the existence of any contract law issues that may adversely impact on the investigation.

(1) The selection of the procurement fraud attorney/organization to provide legal advice on a particular case should be based on the following factors:

(a) The Army activity that provides legal advice to USACIDC.

(b) The Army activity that awarded the contract.

(c) The Army activity responsible for the administration of the contract.

(d) The Army activity that has responsibility for the coordination of remedies under DoD Directive 7050.5.

(e) The DLA region administering the contract.

(2) Legal advice can be obtained from any one of the following activities depending on the circumstances of the investigation. As an example, in a defective pricing investigation, a legal review could be obtained from the office which provided legal advice to the procuring contracting officer, or the designated procurement fraud advisor from the activity concerned.

(a) OTJAG, PFD.

(b) Appropriate local procurement fraud advisor (PFA).

(c) PFA for the Army Materiel Command (AMC) or subordinate commodity command.

(d) PFA for the USACE, or appropriate corps division/district.

(e) PFA for the Military Traffic Management Command (MTMC).

(f) PFA for the U.S. Army Information Systems Command (ISC).

(g) USACIDC attorney advisor for economic crime.

(h) Qualified USACIDC major subordinate command staff judge advocate.

(i) PFA for Defense Contract Management Command (DCMC) region.

(j) Any other appropriate MACOM or subordinate command PFA.

10-15
Referral to the DOJ or a USAO

After the USACIDC supervisory review has been completed to ensure that all appropriate investigative action is being taken and that the case has been reviewed to ensure that there are no accounting and or legal issues that may adversely impact on the investigation, a referral to DOJ or a USAO will be made if appropriate.

a. The determination of whether to refer a particular investigation to a USAO or directly to DOJ will be based on the following factors:

(1) Venue.

(2) Staffing and capabilities of the local USAO, the PFD, Criminal and Civil Division, DOJ.

(3) The ability of the USACIDC office concerned to adequately support the investigation in a particular jurisdiction.

(4) Potential recovery of damages under the Civil False Claims Act.

b. All USACIDC activities are reminded of the provisions AR 27-40, that the referral of a case for civil fraud recovery is to be made through the PFD, subsequent to a review by the procurement fraud advisor and the preparation of a litigation report.

10-16
Reporting of screened cases

The following information will be reported through the USACIDC major subordinate command to HQUSACIDC, ATTN: CIOP-COP-CO for each major contract accounting fraud case screened:

a. Sequence/ROI number.

b. The name of the corporation.

c. The name of the individual subjects.

d. Date of receipt by CID.

e. The nature of the allegation.

f. Source of the allegation/referral.

g. The supervisory agent conducting the review.

h. Disposition of the investigation following the screening and supervisory review to include:

(1) If the allegation was returned for additional investigative work prior to referral to DOJ or USAO.

(2) If the allegation was referred to one of the listed audit activities for further audit work prior to referral to DOJ or a USAO. If so, identify the agency and purpose.

(3) If the investigation is being/has been referred to the DOJ or a USAO.

i. The name, organization and phone number of the attorney conducting the legal review.

10-17
General

Economic crimes normally have as their primary purpose the obtainment of money, property, services, or the creation of some intangible benefit, to which the perpetrator is not legally entitled, and will enhance the individual’s position within industry, or government. Frequently termed the "silent crime," economic crime in most cases requires extensive proactive efforts, rather than the reactive mode to which most law enforcement endeavors are pursued.

10-18
The ECTA

a. The USACIDC economic crime effort must be directed toward the prevention, detection and investigation of criminal activity which results in the loss of Army assets. The most effective employment of the USACIDC's limited assets can only be accomplished by identifying and assessing the specific threats within a CID organization's AOR. The threat assessment process is the most important aspect of the proactive effort, not only in relation to economic crime but also to LOGSEC operations, drug suppression, crime prevention efforts, and personal security vulnerability assessments (PSVA). Without clearly identifying and recognizing the

threat to be countered, there can be no logical basis for an effective proactive effort. Therefore, without a valid threat assessment, any success in preventing or detecting criminal activity would be coincidental.

b. The ECTA process consists of five distinct phases.

(1) Target identification

(a) The initial step in developing an ECTA involves the identification of all potential economic crime targets. A target is any activity, organization or function which is or may be susceptible to economic crime. This can be accomplished through the review of local telephone directories, organizational charts and wire diagrams; and coordination with appropriate installation staff elements.

(b) Target identification should be accomplished for all Army installations, satellite activities, separate Army organizations and MACOMs. A listing of these targets should be prepared by each appropriate USACIDC element.

(2) Information collection

(a) Information will be collected and developed on each identified economic crime target. When several economic crime targets fall within a major activity, they may be consolidated into one file. When information on several economic crime targets is consolidated into a single file the information shall be cross referenced to allow identified information on specific consolidated targets to be retrieved. All criminal information developed on a specific targeted activity will be included in the office's criminal intelligence files. As additional economic crime targets are identified, or as specific threats are recognized and/or resolved, identified economic crime target priorities will be periodically updated to reflect changes in the threat level.

(b) The economic crime raw data file, initiated on a monthly or quarterly (for smaller CID offices) basis, will serve as the conduit through which information is channeled on specific targets. All criminal information developed on a target will be indexed, cross referenced and maintained in the unit's criminal intelligence files.

(c) A locally prepared economic crime target analysis work sheet will be developed for each identified high and medium priority target. This work sheet will serve as the source document for the preparation of the annual ECTA. The work sheet should describe facility/activity, MACOM, function(s), impact on combat readiness, threat potential, criminal intelligence summary, external agency information summary (IG, AAA, DCAA, PFA, PMO, and etc.), susceptibility to economic crime, and special considerations. The work sheet should be unique to their AOR. The work sheet will normally only be updated once each year and should not be enclosed with the ECTA.

(3) Information analysis and correlation. When operationally feasible, information that is developed on high and medium economic crime targets will be reviewed on a monthly basis by appropriate supervisors. The SAC at a minimum should conduct a review of all such files on a quarterly basis. All developed information will be correlated with other internal USACIDC files that pertain to the targeted activity.

(4) Threat assessment

(a) The threat to each identified target is assessed to determine the urgency and level of USACIDC support required.

(b) The assessment will be based on the following considerations, listed in order of importance:

1. Impact on combat readiness.

2. Risk to personal safety of military personnel or DA employees or severe property damage.

3. Susceptibility to criminality, based upon USACIDC records, files and reports, and reported weaknesses identified by other agencies or sources.

4. Financial Threat Potential (FTP), determined by the dollar value of cash on hand, inventory or equipment controlled, contracts, or services provided.

5. Efficient use of USACIDC resources, to include availability of appropriate technical expertise.

6. Requests from supported commanders.

(5) Target Prioritization. Targets are assigned a priority rating of high, medium or low. Dollar value thresholds are enumerated in the definitions of these ratings as a means of clarification. However, they are to be used as a guide only, and must be used in conjunction with other considerations.

(a) A rating of high is assigned to those targets where the threat has a direct impact on combat readiness or safety issues, and where there is information to believe that criminality is imminent, based upon USACIDC findings and information from reliable sources. High priority targets may also have a significant FTP, normally in excess of $100,000. In arriving at a determination that a target will receive a high rating, the dollar value of the activity should not be the only factor in making that determination. Such a determination should be based upon the vulnerability and criticality of the activity that is being targeted. The gold and jewelry in an AAFES activity is vulnerable to theft, but it is not

critical to the Army's preparedness to deploy; whereas the property maintained by a Division Materiel Management Center (DMMC) may not only be vulnerable to theft but it is also critical to the division's combat effectiveness.

(b) A rating of medium is assigned to those targets where the threat has a direct impact on combat readiness, and where there is a reasonable belief that criminality is about to occur or likely to exist. The rating would also be assigned to targets where the threat has an indirect impact on combat readiness, but criminality is considered to be imminent. Medium priority targets also have a moderate to significant FTP, normally in excess of $50,000 but less than $100,000.

(c) A rating of low is assigned to all other targets. As a rule of thumb, the FTP for low priority targets is less than $50,000.

10-19
The ECTA process

a. The focus of the ECTA process will be determined by the special agent-in-charge and operations officer based on the threat, available investigative resources, investigative priorities, and types of crimes that normally occur in the AOR. A sample threat assessment can be found at figure 10-2. At the beginning of each calendar year, a sequence number ECTA file should be initiated to review the previous year's ECTA, analyze new information, and to update target priorities as necessary. The ECTA file should remain open throughout the year to collect information for later reevaluations of target priorities. Changes to target priorities can be documented in a memorandum to include the rationale for the changes. A determination can be made to update the ECTA every 2 or 3 years because the supervisor is fully aware that no significant changes will occur in the AOR. Decisions concerning the ECTA process and update interval of the ECTA should be documented in a memorandum by the special agent-in-charge explaining the rationale for the decisions.

(1) The ECTA should not involve a burdensome, comprehensive fact/issue finding review, but may simply be an update of the previous ECTA.

(2) Economic crime, logistics security, personal security, and drug suppression are areas in which a threat assessment can be conducted. Drug suppression threat assessments will be prepared in accordance with chapter 13 of this regulation. Personal security vulnerability assessments (PSVA) will be conducted in accordance with chapter 16 of this regulation.

b. A separate ECTA may be prepared for each Army installation or site within the AOR if deemed appropriate. Army activities that are located on the supported installation and are within the AOR of the supported USACIDC element should

be included in the ECTA. Tenant activities will normally be included in the installation ECTA; however, activities with a widespread, large scale, geographical location and/or significant operation may be reported by a separate ECTA. The 701st MP Group and its subordinate elements may conduct ECTAs on all activities which are categorized as being above the installation level. The 701st MP Group may also assess major systems acquisition targets, centralized Army acquisition targets, USACE military construction and civil works targets. The installation CID offices may conduct assessments of those service and support contracts and other activities that are unrelated to the 701st MP Group mission.

c. U.S. Army Reserve Component (RC) CID elements should prepare an ECTA of RC facilities.

d. Distribution of the ECTAs will be to the next higher headquarters (i.e., battalion or field office). Distribution by RC CID elements will include the action USACIDC battalion or field office which has training responsibility for the element. The originating office will maintain the original document(s). The next higher headquarters has responsibility for operational review of the ECTA, and should report significant economic crime threats to the USACIDC major subordinate command and HQUSACIDC, ATTN: CIOP-COP-CO. The review will also be used in developing and enhancing the economic crime program in their AOR as deemed appropriate.

e. Since the ECTA represents a strategic criminal intelligence overview, it will not be distributed outside CID channels. Relevant information concerning the economic crime threat should be discussed with the responsible commander or supervisor, and if deemed appropriate, extracts from the ECTA may be provided by separate memoranda.

10-20
Target analysis files (TAF)

a. The TAF is a proactive approach used to address priorities identified during the ECTA process. It should not be considered a preliminary inquiry or significant data file which are initiated based on the receipt of specific information. Unlike the preliminary inquiry or significant data file, the TAF is conducted in an effort to develop more information about a particular facility or activity when sufficient intelligence is lacking. Each TAF will be assigned a separate sequence number.

(1) The TAF is an aggressive proactive investigative effort based on limited or fragmentary criminal intelligence indicators of criminal activity. The analysis effort should, however, be controlled by an investigative plan which is developed prior to the initiation of the effort. There are four primary steps in the conduct of a TAF. These steps are:

(a) Activity identification. During this phase of the TAF, the activity is fully identified. The mission statement is documented in a clear manner which is understandable to an individual not familiar with the activity analyze d. A description of the services provided by the activity is prepared which describes what services are performed, what support is required for the activity to be able to accomplish these services, and what areas are most vulnerable to the criminal threat in the eyes of the facility or activity manager.

(b) Source development. The second step of the analysis process could be the most important of all. Sources must be developed in the early stages of the analysis to allow for the proper targeting and collection of intelligence pertaining to the facility. Upon development of a source, he or she should be questioned to determine any potential problems. Additionally, the source should be initially targeted towards those areas the agent perceives as being most vulnerable as the result of his or her initial assessment of the activity being analyzed. The development of sources should be a continuous process throughout the conduct of the analysis.

(c) Collection and analysis. This portion of the analysis is the substance of the action. During this phase, sources are targeted for specific information, and the various activities of the facility are analyzed to determine which require the highest level of attention by USACIDC concerning the potential for criminal intervention. Crimes which have occurred but gone unreported are identified and conditions conducive to criminality are documented.

(d) Determination of action. Anytime throughout the conduct of the TAF, a determination for further action can be made. If indicators of criminal activity are identified, they need to be reported. If crimes have occurred but have not been previously reported, they need to be investigated. The TAF is used as a "screen" to capture such information. When these conditions are identified, then the appropriate course of action should be taken. Separate files are initiated based on information developed during the conduct of the TAF. If information is developed indicative of a crime within USACIDC purview, then a preliminary inquiry should be initiated and controlled under a separate sequence number. If conditions conducive to criminality are identified which justify the conduct of a CPS then the CPS should be initiated and controlled under a separate sequence number. Note: A CPS may be initiated directly from information not developed from an open TAF, such as from a ROI or source information. Figure 10-1 depicts the economic crime file opening process.

(2) If intelligence is developed which should be reported in a Criminal Information Report (CIR), then a separate sequence number should be utilized to dispatch that report. Under normal conditions the controlling sequence number of the TAF should not be utilized to report information outside of the USACIDC office conducting the analysis.

b. Developing a timetable for the initiation of a TAF on identified targets provides a mechanism to prioritize significant information that would normally require the immediate initiation of a sequence number. This permits the operations officer/SAC to identify the most significant vulnerable and critical areas and to develop a timetable for their analysis. Any such timetable is flexible and will allow for changes throughout the year.

c. The selection of targets should be specific and narrowly defined. A TAF should target a specific area, contract, contractor, logistics activity, individual, and etc. It focuses on a particular entity to gather more information.

d. A TAF will be initiated on those priority activities where criminal information is developed which is indicative of a threat or potential threat. The TAF will be controlled by a sequence number.

e. When appropriate, preliminary investigations, reports of investigation, CPSs and criminal intelligence reports developed as the result of a TAF, will be initiated using separate files. Regardless of the action(s) generated, the economic crime threat assessment work sheet will be updated and the results of the TAF will be recorded in the appropriate criminal intelligence system used at the investigating office.

10-21
TAF scheduling

a. A projected TAF schedule of areas of interest will be formulated on an annual basis and updated semiannually. This schedule is intended to be a management guide for programming activities and work effort throughout the year, especially when coordinating efforts with external agencies such as AAA, IG, etc. Identifying an area of interest on the TAF schedule does not mean that a TAF will be initiated. It means that it is an area of interest that will be looked at and evaluated by means of TAFs, significant data files, and analysis of criminal intelligence to determine if there is a basis or need for initiating some type of further investigative activity. This activity may take the form of a crime prevention survey, a report of investigation, a criminal intelligence report, or any combination thereof, as deemed appropriate.

b. In developing a TAF schedule, the CID supervisor will accomplish the following:

(1) Program command directed assessments that may be announced by HQUSACIDC into the installation TAF schedule, coordinate and supervise all necessary effort, and ensure timely completion to meet established suspense dates.

(2) Identify potential TAF topics from the annual ECTA, ensuring that as a minimum all high priority target areas are scheduled for review and investigative scrutiny as available investigative resources permit. Depending on workload and available resources, medium and/or low threat targets may also be considered for scheduling.

(3) Work closely with the installation crime prevention council, the provost marshal, and the installation commander to identify TAF topics of local command interest.

(4) Ensure continuous evaluation of criminal intelligence, raw data, inspection reports, military police reports, ROIs, which allow for adjusting the schedule and priorities or for identifying the need for unscheduled TAF activity.

c. The conduct of TAF activity will be based upon the availability of personnel resources and priorities. Schedules developed for TAFs must be flexible to allow for changing priorities and unanticipated requirements. Proposed TAF schedules should not be so expansive as to obviously be unworkable or unmanageable. The schedule should be a reasonable assessment of the problems and resources to provide a workable plan while still allowing for unscheduled or unprogrammed activity and changing priorities.

d. While it is not intended that any quota or specific workload requirement be established, it is important to ensure that all working special agents are actively involved in and supporting the organization's TAF program.

10-22
Fraud awareness briefings

a. In order to provide an awareness of fraud, waste and abuse throughout the supported community, USACIDC resources must be actively engaged in a briefing program. Individuals or activities vulnerable to economic crime, based upon the ECTA, will be provided periodic briefings. These include the following functional areas: contracting; cost and pricing; quality assurance; logistical activities involved in the requisitioning, receipt, storage, transportation, accounting, and issue of supplies; and USACE. Fraud awareness briefings should also be presented to officer and NCO professional development classes at the brigade and battalion level. The briefing must focus on issues relevant to the audience.

b. Fraud awareness briefings provide an excellent mechanism for the recruitment of sources and the development of criminal intelligence.

10-23
Special investigative operations

a. Economic crime investigative activity is often well suited for "special investigative operations." For purposes of this regulation, "special investigative operation" refers to an investigative effort or endeavor which requires some form of special handling or effort, beyond what is normally required in a typical criminal investigation. Examples of special investigative operations include:

(1) Covert operations. In certain circumstances a covert operation may be the only way to collect evidence to substantiate that criminality is occurring, or to identify perpetrators.

(2) Sting operations. A form of covert operations, a "sting" involves a store front or business used to attract and identify the criminal element. All sting operations must be carefully planned and approved by the appropriate commander or director dependent upon the level and duration of the sting operation.

(3) Semi-covert operations. These are similar to covert operations, except that the agent or source is not employed in a full time covert role. They are appropriate when the scope of criminality does not warrant a dedicated, full time effort.

(4) Task force and joint operations. A task force is a group of two or more individuals assigned to conduct an investigation. There may be joint efforts with other investigative organizations, and may include additional expertise, such as attorneys or auditors. There is no limit on the number of people who may participate in a task force. The following should be considered prior to initiating or participating in a task force.

(a) The complexity and anticipated duration of the operation.

(b) The impact on other operations if personnel are diverted to the task force.

(c) The level of threat the targeted criminality poses to the Army.

(d) The realistic results which can be anticipated.

(e) Development of special written instructions at the beginning of the operation, detailing the mission, command and control, required support, milestones, and utilization of team members. Guidance may need to be revised and updated as the operation progresses.

b. Special investigative operations may involve the use of one or more of the following:

(1) Technical Listening Equipment (TLE). TLE will be used according with AR 190-53, CID Supplement 1 to AR 190-53 and paragraph 5-34 of this regulation. The use of TLE may be the only way to gather necessary evidence to substantiate allegations in certain investigations. The use of TLE is encouraged where appropriate and is further discussed in Chapter 23 of this regulation.

(2) Sources. The use of sources is one of the most basic investigative techniques. Yet it is often overlooked. Source development, utilization and management are highly important aspects of economic crime investigations and must be aggressively pursued.

(3) Confidential (Limitation .0015) Funds. The use and handling of confidential funds is detailed in AR 195-4. The use of confidential funds in economic crime investigations is particularly effective to identify a market or outlet for stolen/diverted goods, to pay bonuses for information, and to pay sources.

c. Planning any special operation is the most crucial aspect and a written operations plan should be prepared.

10-24
LOGSEC operations in support of Army deployments and exercises

a. The USACIDC's LOGSEC mission includes peacetime operations. The conduct of LOGSEC operations during Army exercises will prepare USACIDC for LOGSEC during deployments and in the combat environment.

b. Each Army exercise is unique, with different missions and several unique scenarios. The LOGSEC support to these exercises must be tailored to the specific exercise.

c. All USACIDC support to field exercises generally comprises three phases:

(1) Preplanning phase. It is during this phase that the USACIDC is notified that its support is required. Usually, the exercise will still be in a planning and development stage. The following steps should be accomplished:

(a) Determine the exact mission of the exercise, where the exercise will be conducted, its length, who is going where, and what will be utilized.

(b) Determine who will be involved in the planning and conduct of the exercise.

(c) Determine what equipment and supplies will be purchased by contract.

(d) Determine USACIDC resource requirements.

(2) Planning phase (pre-deployment). Personnel selected to support the exercise will participate in this phase. The planning phase will be accomplished in a manner similar to a threat assessment, utilizing the following steps:

(a) Coordinate with exercise commanders and facilitators, and provide them with a briefing concerning the USACIDC mission and role during the exercise.

(b) Determine what items are the most critical to the success of the exercise (e.g., personnel, units, major items, spare/repair parts, and other classes of supplies, transportation, etc.), and the disposition of sensitive items subject to pilfering.

(c) Determine when, where and how movements of resources are to be accomplished. Identify the weakest link(s). Designated USACIDC special agents should be present during the loading and unloading of equipment and supplies at the division, brigade, battalion and company level. The decision as to what level will be looked at will be made by the USACIDC office commander/SAC based upon available resources and other operational considerations.

(d) Conduct a criminal intelligence check of personnel, units, locations, suspects, and etc., as needed. Include reviews of the economic crime criminal intelligence system, local police checks, and USACRC name checks, where appropriate.

(3) Conduct phase (deployment). If the preplanning and planning phases have been properly coordinated and validated, the conduct of the mission should be rather routine. The following efforts should be accomplished:

(a) Conduct a logistics security threat assessment and/or threat assessment for priority targets.

(b) Develop, prepare and disseminate CIRs.

(c) Identify other targets as dictated by mission changes and needs.

(d) Conduct of investigations as appropriate.

(4) Post conduct phase (redeployment). This is the conduct phase in reverse, that being the return to home station. Guidance in (3) above applies in this phase.

d. The senior participating agent in a field exercise will prepare an after action report critiquing the exercise and USACIDC involvement. A copy of this report will be provided to HQUSACIDC, ATTN: CIOP-COP-CO.

10-25
Economic Crime References

a. Economic crimes references consisting of Army and DoD instructions, directives, regulations, manuals, pamphlets, MACOM directives, and other publications which provide information or policy are made available on the internet or the CID intranet. All CID agents should obtain and maintain access to Army Knowledge Online (AKO) and CID Intranet in order to access, study, review and research information concerning economic crime and logistic security topics.

10-26
The Army crime prevention program

AR 190-13, Department of the Army Physical Security Program, requires commanders to establish a crime prevention program within their respective units. It also requires that the commander implement a program that will minimize the motivation and opportunity for personnel to commit criminal acts. The contributions of law enforcement personnel are essential aspects to the commanders program. While the basic mission of USACIDC is the investigation of serious felony crimes, a direct relationship between that mission and crime prevention exists. The CPS program is a key element of the overall crime prevention program USACIDC must establish. All USACIDC crime prevention efforts will be planned, coordinated, executed and reviewed in light of their overall contribution to Army and installation/community crime prevention programs as outlined in

AR 190-13. The USACIDC field element commanders should be members of installation/community crime prevention councils or other similar groups constituted to advise commanders and coordinate the local crime prevention effort. Information derived from CPSs should enable USACIDC element commanders to offer this council numerous suggestions in the area of crime prevention and deterrence.

10-27
USACIDC CPS program

a. As a component of the Army Crime Prevention Program, the USACIDC CPS Program will be directed toward identifying findings that are regulatory deficiencies that may be conducive to the loss of Army assets through criminal activity. The CPS will, through the formulation of observations, identify situations that are not procedural deficiencies, but could if left unchecked result in the loss of Army assets through negligence, systemic weakness, or result in the failure of established internal controls. Both findings and observations will assist the supported commander in deterring and reducing crime.

b. All CPSs should be coordinated with supported commanders and other inspection agencies; however, there may be instances where this is neither desirable nor appropriate. Rationale for not coordinating a CPS with a supported commander will b e documented in the case file.

c. Timely completion of the CPS is of utmost importance. The analysis should normally be completed within 90 days of initiation.

10-28
Conducting CPSs of USAR, ROTC and ARNG facilities

All USACIDC elements are authorized to conduct CPSs of selected USAR/ROTC/ARNG facilities/activities consistent with CID workload and capabilities. All CPSs of USAR/ROTC/ARNG facilities/activities will be conducted only after adequate coordination has been completed and the requirement for CPS is established. The criterion also applies to USAR/ROTC/ARNG facilities located on active Army installations. Requests from USAR/ROTC/ARNG facilities/activities for CPS support from USACIDC elements will be submitted in writing through appropriate U.S. Army Reserve Component or ROTC channels to the Commander, USACIDC, ATTN: CIOP-COP-CO. If a CPS is authorized by the Commander, USACIDC, the local CID commander will program the CPS for completion at his earliest convenience as dictated by the CID workload and availability of CID resources. Any CPS of USAR units may also be conducted by reserve CID special agents.

10-29
Preparation for conducting the CPS

Preparation for the actual conduct of the CPS should include the following:

a. Evaluate the complexity of the facility that will be the subject of the CPS. Consider agent knowledge of the facility or type of operation, the need for research, collect reference material and take other measures necessary to ensure a greater level of awareness and proficiency prior to beginning the CPS.

b. Determine the scope of the CPS. It may be advantageous to examine specific functions within an activity rather than the entire activity. Limited scope CPSs are often more appropriate when dealing with large scale activities. The decision concerning the scope should be made during initial planning and evaluation stages of the CPS process.

c. Consider special requirements of the activities which are covered by separate regulations such as AAFES (AR 195-7); DLA (AR 195-8); and The Defense Commissary Agency, and review the pertinent regulations for requirements before proceeding with the action.

d. Determine the need for outside technical skills. If personnel with special skills, such as accounting, engineering, etc., are required to support CPS activity, those agencies tasked to provide the support must be coordinated early to ensure availability of personnel. The personnel utilized need to be briefed on the aims, objectives, and needs for their skills and talents.

e. Determine need for covert status. If placement of a covert operative in the facility before or during the CPS activity is necessary, required authorizations and approval must be obtained from the USACIDC major subordinate commander. Plans for introduction and placement of the covert agent into a facility must be closely coordinated to obtain the desired result without compromise of identity.

f. Preparation of an investigative plan is essential to enhance overall performance. A good plan will provide guidance and direction to the effort and help keep original goals and objectives in mind.

10-30
Initiation of the CPS

It is incumbent upon the CID supervisors to determine at which point the targets on the TAF schedule will be assigned a CPS and, if appropriate, when the results of the CPS indicate that a separate ROI be initiated. Action on a CPS target may begin as a TAF, a significant data file, or raw data file entry, thereby allowing time and the opportunity to further develop information on a targeted facility or activity, and to cultivate sources of information. At the point where the CID supervisors determine crime conducive conditions or discrepancies exist, then the actual CPS will be initiated. If the TAF or other action does not result in the development of any indicators of criminal activity or other findings, the n the matter will be closed as appropriate, without initiating a CPS or other investigative activity.

10-31
Entrance briefing

At the beginning of the overt phase of every CPS an entrance briefing must be conducted with the commander or activity chief or other officials, as appropriate, such as the security officer, site manager, etc. This interview should ad-dress the following:

a. The basis for conducting the CPS.

b. An explanation of the purpose of the CPS and its application to the facility being surveyed.

c. The intended scope and approximate duration of the CPS.

d. The personnel who will conduct the CPS.

e. Other agencies (IG/AAA/PM) who may have an interest in the CPS effort.

f. Request for administrative assistance or support required.

g. That the commander will be informed immediately if any evidence of criminality is discovered during the CPS and subsequent actions required to ensure prompt reporting and investigation of serious irregularities. If this notification will compromise an ongoing investigation, the provisions of AR 195-2 will be followed.

h. That an exit briefing will be conducted at the conclusion of the CPS.

i. That the CPS is designed to assist the commander in fulfilling his responsibilities for crime prevention.

10-32
Investigative activities resulting from the CPS

Normal investigative techniques should be used during the conduct of CPSs. Specific criminal acts detected during the CPS will be investigated. Development of criminal intelligence, not appropriate for inclusion in the report, should be documented and forwarded in accordance with chapter 18 of this regulation.

a. Records check. Results of records checks on key employees of the surveyed facility alerts the commander to potential personnel weaknesses which could result in vulnerability to criminal activity.

(1) During the initial stages of the CPS, data on key personnel who have a direct relationship to the CPS effort will be collected and forwarded to the Crime Records Center for records checks. Local records checks should also be made with the military police, local police, and other agencies as appropriate. Additionally, a review of the employee personnel files should be made as such files often contain information relevant to personality or character traits that could indicate unreliability, susceptibility, or vulnerability toward criminal activity.

(2) Limited investigations of other personnel, such as lower level employees or those acting as agents for key personnel, may be necessary to determine reliability. These records checks will be limited to those performing duties in which their compromise could result in losses to the government.

(3) Information obtained from records checks will be carefully evaluated prior to any dissemination. This type of information will be provided only to the commander or his security officer, or to responsible commanders at higher level s of command. The information will normally be orally briefed, however, if this is impractical, a brief memorandum may be prepared.

(a) Any derogatory information released must be directly related to the performance of duties or position of trust granted to the individual by virtue of his employment.

(b) The information should include adjudications of guilt, when known.

(c) The information should not include subject listings within ROIs completed in the distant past, provided the individual has maintained an unblemished record since that time and there is no direct correlation between previous criminal conduct and the duties performed now.

(d) In any questionable situation, guidance on release of information should be obtained from the supporting staff judge advocate.

(4) Results of records checks will only be referenced in the report in general terms, i.e., "crime records checks revealed derogatory information concerning employees of ...." Specific numbers of employees and offenses should not be used as this may tend to identify the individuals concerned. The report will also identify to whom the information was released.

(5) Information developed on firms/establishments on records checks and background investigations will be handled in the same manner as the release of information concerning individuals.

b. Use of checklists. The use of checklists is encouraged only to the extent that they serve as a reminder to the agent to inspect, observe, or comment upon specific aspects of an operation. Copies of checklists used will not be attached to o r referenced in the CPS report, but will be retained in the case folder. Caution must be exercised to ensure that CPS activity does not become "checklist oriented" to the extent that CPS activity becomes stereotyped and repetitious. Checklists are no t a substitute for good preparation, training, or planning. This is not applicable to the use of checklists developed for use in the personal security vulnerability surveys.

c. Use of .0015 funds. The expenditure of .0015 contingency funds is authorized and encouraged in the conduct of CPS activity in the same manner as in a criminal investigation. The use and expenditure of .0015 funds will be in accordance with AR 195-4.

d. Coordination and integration of inspections. All CPS efforts should be coordinated and integrated with other DA agencies and activities charged with similar inspections responsibilities, such as IG, AAA, DCAA, and military police. The purpose of such coordination is to reduce the total number of inspections/CPS commanders receive during any one year. Commanders who are repeatedly subject to inspections/CPS from various agencies may view such actions as harassment rather than assistance. Proper integration of these efforts and the conduct of joint activities, will result in reports that are more thorough and meaningful to commanders.

(1) Coordination with AAA/IG. All USACIDC elements will establish and maintain continuous coordination with AAA and IG personnel. Coordination and exchange of information is essential during planning phases of the CPS. A USACIDC element might conduct a CPS on a facility which is subject to IG inspections or AAA audits, therefore information on results of prior audits/inspections and any other background information known to these other agencies would be beneficial during the conduct of the CPS.

(2) If both USACIDC and AAA have scheduled CPSs/audit of the same facility during the same time period, consideration should be given to conducting a joint effort. The USACIDC field element commander scheduling the CPS will coordinate the recommendation for joint effort with AAA. Known criminal activity and criminal information used in scheduling the CPS is a significant factor to be used in making a decision for a joint action or for one agency to defer to the greater interest o f the other agency, necessitating the cancellation or rescheduling of the CPS or audit. Normally a six-month separation of CPS/audit activity should be the minimum period considered when rescheduling such activities.

(3) When simultaneous CPSs/audits are to be conducted, consideration should be given to having one entrance briefing attended by both AAA and USACIDC personnel. The USACIDC should not proceed further until AAA has examined the facility in sufficient detail as to identify any weaknesses indicating the possibility of criminal activity or other crime conducive conditions. Records checks, research, and other such background activities should be performed in preparation of the USACIDC portion of the joint effort during this period. In any event, the CPS will be separate and distinct from the audit, but will focus upon any areas identified by the audit team to be an area of potential criminal activity. The exit briefing should also be conducted at one time with both AAA and USACIDC personnel being present.

(4) When a joint effort is not conducted, there may still be a need for AAA assistance. Requests for special audit assistance estimated to require ten man-days or less will normally be submitted in writing by the applicable USACIDC major subordinate command to the appropriate AAA district manager. The request will include all pertinent information such as type of facility being surveyed and the anticipated scope of the audit effort. If time is of particular concern, the request may be made telephonically. Requests for AAA assistance in excess of ten man-days must be submitted to this HQUSACIDC, ATTN: CIOP-COP-CO.

(5) Coordination with provost marshals. Joint conduct of physical security inspections and CPS will be undertaken whenever possible. This will be based upon mutual resource availability, scheduling adjustments, the criticality/vulnerability of the facility and previous inspection/CPS reports. Generally, physical security officers should make physical security specialists available so as to conduct joint inspections current with the CPS. Although many inspections will be conducted jointly, each team will accomplish its portion of the effort according to its own procedures and neither will direct the activity of the other.

(a) Joint efforts will consist of close coordination during pre-inspection/CPS planning to ensure that the efforts of each team are mutually supporting. One entrance briefing with representatives from both the physical security inspection/CPS team will be conducted. Redundancy and duplication of effort should be avoided and the efforts of each team should compliment the other.

(b) Separate reports will be prepared at the conclusion of the inspection/CPS. Normally the physical security inspection will be completed prior to the CPS, therefore, the exit briefings need not be conducted concurrently; how ever, the agent conducting the CPS should arrange to be present during the exit briefing conducted by the physical security specialist.

e. Furnishing CPS results to commanders. Commanders will be kept informed of the status of the CPS in which they have an interest. This may be done verbally during the course of the CPS or by furnishing the commander with an interim CPS report, if appropriate. The forwarding of information in this manner ensures that supported commanders are afforded the maximum opportunity to initiate timely corrective actions.

10-33
Exit briefing

At the conclusion of the CPS, after the findings have been thoroughly reviewed and coordinated with other agencies assisting in the CPS, an exit briefing will be conducted for the commanders, activity chief, or other officials, as appropriate.

Upon the completion of a CPS of commissaries, the appropriate Defense Commissary Agency (DeCA) field office should be afforded the opportunity to have a representative present during the briefing. Exit briefings should include:

a. Information as to the scope of the CPS, personnel who conducted the CPS, and other agencies involved in the effort.

b. The findings and recommendations that will be listed in the final report must be presented in sufficient detail to provide the commander with an accurate appraisal of the conditions within the facility. The distinction between findings and subjective recommendations should be clearly articulated to the commander to ensure that he understands that there is no requirement to respond to subjective findings. Subjective findings are provided for action deemed appropriate.

c. Recommended actions to reduce and/or eliminate identified conditions or discrepancies that may contribute to undetected criminal activity should be discussed. Recommendations must present the commander with a reasonable and practical approach for correcting conditions that may result in criminal activity. Such recommendations should be based on the level of the potential threat and potential loss to the government. Unrealistic or overly demanding recommendations that are more costly o r demanding than the threat or potential loss do little to enhance the credibility and effectiveness of the CPS. For example recommending a change in procedures that will result in an annual savings of $750, but cost $6,000 in additional personnel requirements is not realistic. However, this does not mean that the issue should not be brought to the commander’s attention.

d. Inform the commander of the requirement to submit a report of corrective action as required by AR 195-2 and this regulation. A commander requested CPS does not require a report to be submitted (figure 10-5). All CID initiated CPSs do require reports of corrective action. When required, the report of corrective action must be furnished within 90 days after receipt of the final CPS report. The only exception is a CPS of DLA activities which will respond to the CPS in accordance with AR 195-8.

10-34
CPS conducted by CID reserve special agents

All CPSs conducted by reserve CID units conserve the limited resources of this command and provide much needed support to reserve commanders at all echelons. In addition, it assists, by a proactive mode, in identifying potential criminal activity and other systemic problems that could result in the loss of Army assets and accomplishes appropriate corrective action before those problems are brought to the command's attention via the news media, hotline referrals, etc. All CPSs conducted by reserve CID units could be directed by the appropriate

reserve field commander for completion during periods of inactive duty training (IDT). In this connection, CID field elements should maximize use of reserve assets by being cognizant of the following:

a. Reserve special agents of designated reserve units may conduct CPSs during annual training (AT) and/or during IDT.

b. Commanding General (CG), Forces Command (FORSCOM), may select specific sites for a CPS and authorize individual reserve units to conduct the CPS in lieu of other training activities during IDT.

c. The USACIDC field elements can select specific functional areas and locations for a CPS to be conducted by individual reserve units during periods of AT.

d. All USACIDC major subordinate command and subordinate element commanders will support reserve CID units during the conduct of CPSs during IDT. This will include technical advice, on-site assistance and conduct of records check. During AT t his support will include the above, finalization, review, and distribution of reports.

e. Other CPS requirements for reserve units will be specified in letters of instruction (LOIs) from HQUSACIDC.

10-35
CPS reports

a. Many CPS reports are often reviewed by key Department of Army and DoD officials. To ensure that CPS reports achieve the desired results, they must be written in a manner understandable to those not familiar with the activity receiving the CPS.

b. A CID sequence number will be assigned to the CPS. The CPS sequence number shall be a separate number than that assigned to a previously initiated target analysis file, threat assessment, significant data file, or complaint file.

c. A CPS report can include logistics, installations activities, and crime trend analysis.

d. A CPS will not normally be initiated unless there are indications of crime conducive conditions or other problems. These indicators will normally be developed through the ECTA and TAF process.

10-36
Preparation of the CPS report

All CPS reports will be prepared in memorandum format, using letterhead stationary for the first page and plain bond paper for all continuation pages. All pages will be numbered consecutively with the number being centered at the bottom of each continuation page; the first page will not be numbered. The required data and specific format will be accomplished in accordance with the example depicted at figure 10-3.

a. Subject: Enter CID Report - CPS Report Number (to include CID Sequence number, and offense codes).

b. Type of CPS: Enter Installation Activity CPS, Crime Analysis CPS, Logistics CPS, etc., as appropriate.

c. Survey of : Identify the topic, area, or subject of the CPS.

d. Scope: Describe the limits of the CPS effort.

e. Requested by: Identify by name and/or duty position and organization, the individual requesting the CPS. Those initiated by CID elements will use USACIDC duty position and organization only.

f. Conducted by: Enter the name(s) of the special agent(s) assigned to conduct the CPS. All U.S. Army Reserve Component agents will include reserve unit following the name. If more than one agent is listed, the last name of each agent will suffice.

g. Purpose: Describe the intent and purpose or objective of the CPS effort.

h. Criminal activity discovered as result of CPS: This will be followed by a yes or no response, as appropriate. This entry will not be required for Crime Analysis or Personal Security Vulnerability Analysis.

i. Cost Avoidance. If utilized, see paragraphs 10-42 and 10-43 of this regulation for instructions concerning this portion of the report.

j. Entrance briefing: List full name, title, and organization of the senior responsible individual attending the entrance briefing and the date the briefing was conducted.

k. The body of the report. The contents of the report will vary depending on the type of CPS being conducted. Care should be used by the reporting agent(s) to include only significant activity and omit verbosity, trivia, repetitious or

meaningless information. Persons identified for the first time will be fully identified by grade or title, name, job position and unit. Subsequent references will be by last name only and printed in capital letters. The body of the report for logistical/installation CPSs contain the following information and format:

(1) Findings, recommendations and observations.

(a) Findings: Will only identify those regulatory deficiencies that may be conducive to the loss of Army assets through criminal activity. The conditions identified may result from a lack of regulatory compliance, departure from lawful general orders or violations of applicable statues, laws, or prescribed standards. This may result from inconsistent regulatory guidance, inadequate supervision, and/or management procedures. Care must be exercised to ensure that only conditions which are actually conducive to the loss of Army assets are identified in the report. Each finding must be explained in sufficient detail so that the supported commander will readily understand why the identified conditions are conducive to the loss of Army assets. On the spot corrective actions taken by the commander will also be noted after the specific finding.

(b) Recommendations: Will immediately follow each crime conducive condition listed. Recommendations will be discussed with the responsible commander either during the CPS or during the exit briefing. Recommendations should be designed to eliminate or reduce loss of Army assets and may identify the need to change existing regulations or the implementation of new regulations. Recommendations must be based upon common sense and reasonableness of effort, and evaluated by contrasting the level of threat or potential for losses resulting from the continuance of current practices in comparison to the cost of correcting the identified problem.

(c) Observations: Additional information may have been developed during the course of the CPS which identified potential problem areas that fall short of being a finding. Observations will identify situations that were not regulatory or procedural deficiencies, but could, if left unchecked, result in the loss of Army assets through negligence, systemic weakness, or result in the failure of established internal controls. If left alone these areas could develop into an environment conducive to criminal activity. To this end, the agent conducting the CPS should incorporate this information into the report as an observation to inform the action commander of potential problems. When such information is included, it will be clearly identified as an observation and will not require formal response by the action commander.

(2) Summary of related activity: This section of the report, if deemed appropriate, should include a brief summary of pertinent investigative activity designed to clarify a particular matter which will aid in the understanding of the report

l. The body of the crime analysis survey report (figure 10-4) will contain the following information and format:

(1) Problem analysis: This will consist of two paragraphs. The first will describe the specific problem addressed by the survey to include the reason the survey effort is focused on the type of crime identified. This should answer the question as to why this crime is a problem and requires special consideration. A description of the population served (military, family members, and civilian employees), the type of units assigned and other data to describe the area being examined w ill be included. The second paragraph will describe the methodology used in the conduct of the survey. This may include a statistical analysis of criminal activity within a limited time frame, interviews, review of regulations and records, and on the scene observations.

(2) Findings and recommendations: This should be a narrative listing of the results of the survey and the factors which the agent concluded were contributory to the crime problem. This may include diverse conditions, such as, inadequate security patrols, lack of command emphasis, failure to enforce regulations, conduct proper inventories, lack of lighting, or any of a number of other conditions that render the installation/community susceptible to that type of criminal activity being discussed. Statistical data should be detailed in exhibits which are referenced where appropriate. Each condition cited will be followed by a recommendation designed to reduce or eliminate the condition identified.

(3) Summary of related activity: This section of the report, if deemed appropriate, should include a brief summary of pertinent investigative activity designed to clarify a particular matter which will aid in the understanding of the report. This is not intended to be a duplication of information contained in the agent activity summary nor as a justification of time spent on the survey.

m. Exit briefing: List full name, title, and organization of the senior responsible individual attending the exit briefing and the date the briefing was conducted.

n. Exhibits: Exhibits may be appropriate to support the findings of the CPS effort and to enhance the understanding and overall quality of the investigative effort. Exhibits will be listed in the same manner as in an ROI with use of both attached and not attached (referenced) exhibits as appropriate.

o. Status: Identify this as a final or interim report and if a report of corrective action is required from the action commander.

p. Report prepared by: The special agent who prepared the report will sign the report using a signature block positioned near the left margin. The signature indicates the report accurately reflects the investigative activity conducted, that it is complete, and has been prepared according to pertinent regulations, policy, and doctrine. If the agent who prepared the report is also the approving authority,

this entry is not necessary. If the agent is not available to sign the report in a reasonable time, another agent may sign for the preparing agent.

q. Report approved by: The approving authority will sign the report using a signature block, which reflects the approver's name, rank, branch, and title as depicted in the example at figure 10-3. When the approver is a special agent, only the name and title will be used for the signature block.

r. Distribution: The specific distribution of the report will be entered and reflect to whom copies of the report were provided. Distribution requirements are addressed in chapter 8 of this regulation.

s. The final CPS should be uploaded into the ACIRS database under the memo option of the narrative.

10-37
Reporting results of corrective action

a. The originating USACIDC element will establish procedures to ensure that reports of corrective action are received for each CPS report requiring such a response (figure 10-6). This will include follow-up inquiries when the response has not been received within the 90-day suspense period.

NOTE: This does not apply to CPSs in support of DLA. HQDLA will review reports of action taken and forward them to USACIDC for information.

b. In preparing endorsements, the CID element will consider the effectiveness of the action taken by commanders and acknowledge this by remarks in the endorsement. The CID comment will be limited to an evaluation of the action from a law enforcement perspective and will not imply that command prerogative is questioned.

c. If the commander's action is considered inadequate, the matter should be reviewed with the action commander for reconsideration. If the matter cannot be resolved locally and is pertinent to a particularly significant finding, a copy of the CPS with the report of action taken will be forwarded to the appropriate USACIDC major subordinate command for resolution at that level.

d. The report of corrective action will be maintained locally in the case file.

10-38
Supplemental CPS reports

Supplemental CPS reports will be prepared on letterhead stationary using the same basic format of the original report. The subject line will reflect CPS - 1st (number as appropriate) Supplemental - report number. Supplemental reports will be prepared and submitted when new or additional information is developed concerning a final CPS and initiation of a new CPS is not considered necessary.

10-39
Follow-up action

Selected facilities in which numerous crime conducive conditions have been identified should be considered for a follow up action. While it is not reasonable, practical, nor expected that every activity be resurveyed to ensure all conditions have been corrected, CID commanders should ensure that those facilities having significant or persistent problems are scheduled for a follow-up TAF or CPS. The effectiveness of corrective action taken by the action commander must be considered when making the decision to conduct a follow-up action or not. When a follow-up TAF or CPS is appropriate, a new report number will be initiated

10-40
Classification of CPS reports

a. All CPS reports containing national defense information will be classified, handled and downgraded according to AR 380-5. Requests for earlier downgrading or declassification will be submitted to Commander, USACIDC, ATTN: CICG-IN-SC. Full justification for declassification will be provided.

b. Unless a CPS requires special handling due to the sensitive nature of the information in the report, it will be marked "FOR OFFICIAL USE ONLY". Storage, handling, and protection of such reports will be in accordance with AR 25-55 and this regulation. CID reports are exempt from automatic termination of protective markings in accordance with AR 25-55.

c. The CID Form 14 (CID Document Cover Sheet) will be used as needed.

10-41
Release of information

Information generated through the CPS process is the property of USACIDC and release to others will be in accordance with AR 25-55.

10-42
Cost avoidance computation

a. Criminal cost avoidance is not required. Computation of cost avoidance may be utilized to identify meaningful, justifiable and easily understood savings realized by the U.S. Army as a direct result of USACIDC criminal investigations and CPSs. When a potential cost avoidance is questionable, it will not be reported.

b. Explanation: A savings to the U.S. Government which is realized from investigative steps taken by CID that creates a clear and unmistakable dollar savings or identified reduction in overall cost. When a CID report of investigation or CPS identifies a systemic practice which has been subsequently stopped or modified due to some type of CID interdiction, any clear and unmistakable savings to the U.S. government may be reported as cost avoidance.

c. Only those costs which would or could be lost as the result of criminal acts may be reported as cost avoidance. All costs reported as having been avoided because of USACIDC involvement must be calculated logically and reasonably. The cost avoidance must be supportable by sufficient evidence.

d. Expenses associated with authorized wages, benefits, or anticipated retirement program payments will not be included in the determination of criminal costs avoided. Likewise, costs associated with current or anticipated contracts are not a voided as these services or goods will normally still be required. Costs to be included in any calculation of criminal cost avoidance within any USACIDC report is limited to two specific areas:

(1) Costs which would have been incurred by the government if identified criminality were allowed to continue. These may be reported in the ROI.

(2) Costs which could reasonably be expected to occur if conditions conducive to criminality were not corrected. These may be reported in the CPS.

e. Computation of costs. Criminal costs avoided will be categorized in two areas:

(1) One-time costs which are those costs that would have resulted from the commission of one crime had the USACIDC not intervened.

(2) Annual costs which are those costs determined through the extrapolation of one-time costs on an annual basis. If an employee systematically pilfers $2,000 once per month and is apprehended by the USACIDC for that crime, the one-time cost avoidance would be $2,000 and the annual cost avoidance would be $24,000 (12 x $2,000). Annual cost avoidance will be computed only when it can be demonstrated that an identified crime was part of a recurring criminal scheme

or activity. If an individual is apprehended for a theft and there is no evidence that previous related crimes had been committed or were planned for the perpetrator, there will be no computation of annual criminal cost avoidance.

The above example demonstrates the computation of criminal cost avoidance resulting from a crime which had transpired. Cost avoidance can also be calculated from crime conducive conditions identified during the conduct of a CPS, although this can be more difficult. If it can be demonstrated that a condition exists which would allow for the detected loss of funds or property, then a one-time criminal cost avoidance may be claimed. This cost avoidance must be limited to that amount which could reasonably be diverted one-time without being detected and without triggering internal controls. If it is likely the diversion could continue over a period of time at a specific frequency, then an annual computation may be accomplished. The computation would be the one-time cost multiplied by the frequency of occurrence within a one year time period. For example, if it is reasonably certain the crime could be repeated once per month without detection, then the frequency would be 12. Therefore, the equation to reach the annual criminal cost avoidance would be the one-time cost avoidance multiplied by 12. It is imperative that all costs reported as having been avoided be calculated logically, reasonably, and be supported with appropriate documentation.

10-43
Reporting criminal cost avoidance

a. Criminal cost avoidance is not required. Criminal costs avoided as the result of any USACIDC activity may be reported in CPSs and "U.S. Government property/fraud" related ROIs. When a potential cost avoidance is questionable, it will not be reported.

b. In a CPS, criminal cost avoidance may be documented in a separate paragraph immediately preceding the "criminal activity discovered/not discovered" statement. The word "criminal" may be omitted if the cost avoidance is determined to be administrative or procedural costs and no criminal activity was discovered as a result of the survey.

Example:

Criminal Cost Avoidance

One-time: $10,000.00
Annual: $120,000.00

Criminal activity (was/was not) discovered as a result of this survey.

c. In an ROI, the identified criminal cost avoidance may be reported in a separate paragraph immediately following the investigative summary. Example:

Investigative Summary: Investigation disclosed that SMITH stole a total of $200,000 between 1 January and 31 October 1989 by submitting claims, which he knew to be false. On ten monthly claims, SMITH billed the government for five super widgets, each valued at $5,000, which he had not delivered.

Criminal Cost Avoidance

One-time: $25,000.00
Annual: $300,000.00

d. Criminal cost avoidance paragraphs may appear in CPSs and ROIs that relate to government property/funds crimes. The cost avoidance computation method will be described in the Agent Activity Summary (CID Form 28). When costs avoidances are not used, blank cost avoidance lines will not appear in the report. Likewise, if a crime is reported in which there is no evidence of continuing criminality, but as a result of CID investigation there was a clear and unmistakable cost avoidance identified, the one- time only cost avoidance line may appear in the report.

e. The identified savings will also be entered into the ACIRS miscellaneous data field.

10-44
Personnel and training

All USACIDC agents will support the economic crime program.

a. The economic crime program utilizes all of the USACIDC resources at various levels. Basic fraud training is provided at the CID Basic Course at initial entry. Additional training is provided during attendance at the Advanced Fraud Investigation Course (AFIC). It is the goal of USACIDC that all accredited agents attend the AFIC.

b. General prerequisites for attendance at the AFIC are:

(1) At least two years CID military investigative experience or one year civilian CID investigative experience. Waivers may be considered on a case by case basis as determined by CIOP-PP-TR. However, special agents that have not completed their apprentice period will not attend the AFIC. All special agents should be scheduled for attendance at the AFIC prior to their fifth year of accredited service.

(2) Accredited special agents of the active or reserve component in grade E-5 or higher.

(3) Not more than 18 years of military service unless Regular Army warrant, or enlisted with at least two years remaining on current enlistment.

(4) With the prior approval of CIOP-PP-TR, military police officers who are accredited USACIDC supervisors, may attend the AFIC.

(5) Investigators for other DoD or government agencies with a least two years of experience.

(6) Meet the Army's height and weight and physical fitness standards.

c. Local national criminal investigators may attend the AFIC on a case by case basis as determined by CIOP-PP-TR.

10-45
Military economic crime supervisors

a. Select economic crime warrant officer special agents (ASI 9E) will be utilized as team chiefs, SACs and operations officers to provide direct supervision and emphasis to the EC/LOGSEC mission.

b. Training required for agents seeking ASI 9E or who have been selected as economic crime supervisors will be in accordance with AR 611-112. Furthermore, the selectee should have successfully completed two courses listed in the Army Logistics Management College (ALMC) course catalog. The two courses must provide training in acquisition contracting, depot operations, inventory management, reutilization/marketing operations, property accounting, disposal management, contract law, cost analysis, maintenance management, or other related topics which are considered advanced logistics courses to aid in the supervision of economic crime investigations.

c. ASI 9E will be awarded by the HQDA career management authority to qualified warrant officers upon recommendation by the Commander, USACIDC or designated representative.

d. After award of the ASI, agents should complete at least one refresher course in the logistics area per year.

10-46
Civilian education program

a. The Civilian Education Program allows warrant officer special agents to earn a bachelor's degree in Business Administration (BA), or a master's degree in Business Administration (MBA). These are fully funded programs that are available through colleges and universities. Upon successful completion of the BA program, agents can be assigned to a position requiring this education level.

b. The Civilian Education Program is governed by AR 621-1. All applicants must have been accepted by a college or university prior to initiating a Request for Validation of Army Education Requirements Board (AERB) Position, DA Form 654-R, in accordance with AR 350-100. The Total Army Personnel Command conducts an AERB board to select Army military personnel who have requested to participate in the Civilian Education Program.

CHAPTER 11

11-1
General

This chapter provides procedures for the Major Procurement Fraud Units (MPFU). However, installation level CID fraud elements should be familiar with the general contents of this chapter. The nature of MPFU investigations requires additional considerations which may differ from other procedures described in this regulation.

11-2
MPFU structure and operations

The central mission of the MPFU is to conduct investigations of fraud that involve MACOM major acquisition contracts, and USACE awarded and/or administered contracts. Further, the MPFU may conduct other investigations of sufficient complexity, sensitivity or impact through coordination, as required, with other USACIDC elements, or as assigned by higher headquarters. The organizational structure is:

a. The MPFU is an operational element of the 701st MP Gp (CID).

b. The MPFU operational elements consist of fraud field offices and resident agencies.

c. MPFU field elements will be located based on current and projected mission requirements and available logistical support.

d. A MPFU special agent may be assigned as an investigative coordinator at MACOMs to coordinate overall USACIDC investigative support.

11-3
Major procurement fraud investigations

As an integral part of the Economic Crime Program, major procurement fraud investigations are concerned with the protection and recovery of vital Army assets, ensuring the integrity of the Army's capability to perform its combat role.

a. Scope. For the purposes of this regulation, major procurement contracts are those procurements that are initiated by a centralized procurement activity for systems, products, or services for use throughout the Department of the Army (DA) or DoD. Contracts for these items are awarded by the MACOMs. All procurement actions are governed by applicable federal laws, the Federal Acquisition Regulation (FAR), DA and DoD supplementary regulations and

directives, and AR 70-1. These major procurement efforts also include contracts awarded and/or administered by the U.S. Army Materiel Command (AMC), the U.S. Army Corps of Engineers (USACE), and the Military Traffic Management Command (MTMC).

(1) Frauds involving major systems acquisition contracts include the activities of contractors, consultants, and Army and DoD employees. The crime of fraud may occur during the identification of the requirement for a system, service, or product; during the research and development process; or manufacturing phase of the acquisition including the juncture where the system or product enters the Army or DoD inventory and/or accountability is established by the U.S. Government.

(2) The investigation of major systems acquisition contracts will entail significant investigative efforts which are often multi-locational.

(3) Targets include MACOM contracting offices, DA/DoD contractors, and other elements of the civilian-military industrial community.

11-4
MPFU investigative purview

The MPFU investigative purview includes paragraph 10-5 and current governing DoD Instructions and Memoranda:

a. Any matter involving centralized troop support (equipment, supplies, or services) contracts, major systems acquisitions or USACE awarded and/or administered contract(s)/project(s), which result in the delivery of defective products or product substitution where a hazard to personnel safety, health, and/or readiness or combat effectiveness is indicated, regardless of loss or value; or

b. The subject(s) of the investigation include a military officer in the grade of 0-6 and above, or a civilian employee in the grade of GS-15 or above, or a procurement official, regardless of grade, as defined by the Procurement Integrity Act (41 USC 423) and involves centralized troop support (equipment, supplies, or services) contracts, major systems acquisitions or USACE awarded and/or administered contract(s)/project(s); or

c. Criminal corruption (bribery, gratuities, etc.) cases related to procurement that involve current or retired military or DA/DoD civilian personnel who were, or are, involved in any centralized troop support (equipment, supplies, or services) contracts, major systems acquisitions or USACE awarded and/or administered contract(s)/project(s) without regard to dollar loss; or

d. Violations of the Clean Water Act and any matter involving environmental issues resulting from USACE awarded and/or administered contracts for the cleanup of hazardous and/or toxic waste sites at U.S. Government installations, facilities, activities and sites within civilian jurisdictions without regard to dollar loss; or

e. Any matter involving centralized troop support (equipment, supplies, or services) contract(s), major systems acquisitions or USACE awarded and/or administered contract(s)/project(s), which has received, or is expected to receive, or if disclosed, could be expected to receive significant media coverage; or

f. Antitrust violations that involve any centralized troop support (equipment, supplies, or services) contract(s), major systems acquisitions or USACE awarded and/or administered contract(s)/ project(s).

g. Any matter specifically designated by the Director, MPFU, the Commander, 701st MP Gp (CID), and/or HQUSACIDC.

h. Except as otherwise indicated in paragraphs 11-4a thru 11-4g above, the MPFU will normally investigate fraud where the potential loss is $100,000 or more and involves any centralized troop support (equipment, supplies, or services) contract(s), major systems acquisitions or USACE awarded and/or administered contract(s)/project(s). The MPFU may, on a case-by-case basis, coordinate with another USACIDC element to assume investigative responsibility for fraud under $100,000 or may coordinate with the affected USACIDC major sub-command for control transfer to another USACIDC element.

i. USACIDC components receiving information meeting the above criteria, regardless of actual or potential dollar loss, shall promptly coordinate that information with the nearest MPFU office.

j. Those fraud allegations that are not within the criteria established for MPFU shall continue to remain within the investigative purview of the concerned MP Gp (CID) .

(1) Installation USACIDC units will need to distinguish between those construction and renovation project contracts awarded and administered by the local Director of Public Works (DPW) and those which are awarded and/or administered by the USACE.

(2) Investigative support to depots and ports will continue to be the responsibility of the concerned MP Gp (CID), unless the incident meets the criteria established by paragraphs 11-4a thru 11-4h.

l. Disputes involving investigative jurisdiction that cannot be resolved b

11-5
MPFU management responsibilities

a. The Director MPFU will:

(1) Direct the overall operation of the MPFU.

(2) Allocate MPFU assets to accomplish mission needs.

(3) Upon direction from higher headquarters, assist headquarters or other MP Gp (CID) commands in the conduct of economic crime investigations or logistics security operations.

(4) Establish the investigative priorities of the MPFU.

(5) Serve as the principal advisor to the Commander, 701st MP Gp (CID), on all major procurement fraud matters.

(6) Monitor and oversee the planning and presentation of the MPFU training programs.

(7) Provide functional area expertise to the USACIDC IG.

b. The Chief, Operations Division, MPFU will:

(1) Monitor the major procurement fraud program.

(2) Identify major procurement fraud targets based on criminal intelligence from MACOMs, DA and DoD.

(3) Monitor the coordination of all remedies pursuant to major procurement contract fraud investigations.

(4) Conduct in-service training as required.

(5) Conduct field assistance visits to assess the MPFU fraud program.

(6) Assist field elements as directed by the Director, MPFU in obtaining additional technical support for complex investigations.

(7) Establish Standard Operating Procedures (SOP).

(8) Monitor all major procurement fraud referrals from DoD organizations and provide feedback to those organizations, concerning the results of the referral, if requested.

11-6
MPFU field element operational procedures

a. Target prioritization: MPFU field elements will establish and maintain Economic Crime (EC) target prioritization utilizing a combination of the following:

(1) Target collection folders.

(2) Review and Analysis of data.

(3) Criminal intelligence system analysis.

(4) Unit Liaison Program.

(5) Economic Crime Threat Assessment (ECTA) or similar document or process.

b. Crime Prevention Surveys: MPFU elements will not normally conduct crime prevention surveys; however, if conducted, the procedures in Chapter 10 will be followed.

c. Records Maintenance: MPFU elements will establish and maintain investigative and administrative files pertinent to the MPFU mission in accordance with this and other applicable regulations. However, MPFU elements may establish a local policy based upon operational need for investigative files retention that may exceed, but not be less than established USACIDC policy.

d. Investigative Venue: MPFU elements will conduct procurement fraud investigations in the federal judicial district where principal venue exists. Principal investigative venue generally resides in the federal judicial district in which the contractor is located and/or in which the contract performance occurred. MPFU elements will coordinate to determine investigative responsibility in those instances where apparent equal venue exists or is otherwise unclear. Unresolved disputes will be referred to the Director, MPFU for resolution.

e. Investigative Referrals: When a MPFU element develops intelligence or significant data which is within the investigative purview of any other USACIDC element, the information will be expeditiously forwarded to the appropriate CID element.

f. Referral of MPFU investigations: No Army major procurement fraud cases will be referred outside the MPFU without prior approval from the Director, MPFU.

g. An investigative plan will be prepared at the onset of all MPFU case actions except RFAs and RDFs. Investigative plans will be continually updated throughout the course of the investigative process.

h. Provide functional area expertise support to installation level CID field elements.

11-7
Receipt of referrals and development of cases

a. When a MPFU element receives or develops information that a criminal incident has allegedly occurred that is within its investigative purview, a case file will be initiated by entering the information into the ACIRS database. If the receiving MPFU field element does not have investigative responsibility for the allegations, the information will be transmitted to the appropriate MPFU element or other criminal investigative organization.

b. When the MPFU receives formal referrals of criminal allegations from other agencies/organizations, the Chief, Operations Division, MPFU will, by a request for investigation (RFI), task the appropriate MPFU field element to investigate the allegations. The receiving MPFU field element will evaluate the information, conduct a preliminary inquiry, if required, and respond by the RFI suspense date. When a preliminary investigation does not result in the initiation of an ROI, a summary of investigative action in an agent's investigation report (AIR) will be prepared and provided to the Director, MPFU, ATTN: CISAM-OP. This also applies to RFIs received from HQUSACIDC.

11-8
MPFU joint investigative procedures

a. The conduct of joint investigations among defense criminal investigative organizations (DCIOs) is governed by current DoD instructions and memoranda as supplemented by USACIDC policy.

b. The conduct of joint investigations with non-DCIO investigative agencies is governed in some cases by DoD/DOJ memoranda of understanding (MOUs). When no specific agreement governs joint investigations with a particular non-DCIO agency, USACIDC policy will govern (See paragraph 4-12).

11-9
FinCEN requests

MPFU elements are authorized to utilize the Financial Crimes Enforcement Network (FinCEN) in accordance with this regulation and other applicable directives.

11-10
Task force operations

All multi-agency task force participation will be approved by the Director, MPFU, prior to commitment of any resources. MPFU units will participate in task force operations when the facts of the case agree with those factors that will likely result in a significant remedy with substantial impact on the Army.

a. The special agent-in-charge of the fraud field office is responsible for assessing investigations for the appropriateness of forming or joining a multi-agency task force using the following criteria:

(1) Impact on the Army.

(2) Prosecutive merit of the case.

(3) Potential for significant remedies.

(4) Available funding, resources and personnel.

b. The special agent-in-charge of the fraud field office is responsible for submitting a task force proposal to the Director, MPFU, based on the assessment conducted. It will detail the objectives of the proposed task force and outline the anticipated level of MPFU participation.

(1) The proposal will include:

(a) General case strategy.

(b) Task force organization.

(c) Number and type of personnel to be assigned to the task force.

(d) Administrative and logistical requirements.

(e) An estimate of funding for each of the relevant areas.

c. No MPFU element will participate in a multi-agency task force without a memorandum of understanding (MOU) agreed upon by the designated approving official of each participating agency.

(1) The task force MOU should identify the DCIO/Agency that has been designated as the lead agency and the rationale for assigning that responsibility to the designated lead agency.

(2) The senior MPFU agent assigned to the task force will provide written periodic progress reports, as required, through the special agent-in-charge to the Director, MPFU. This report should focus on specific task force accomplishments and identify all adjustments to support requirements, anticipated remedies, task force completion date and an updated investigative plan, as necessary.

11-11
Qui Tam

a. The Federal False Claims Act, 31 USC 3729 et seq, permits Qui Tam, or private citizen, suits. Any citizen (relator) (such as a former contractor employee) can sue, on behalf of the United States of America, a contractor for procurement fraud and personally receive a percentage of the damages.

b. Qui Tam matters having Army interest are filed by the relator in Federal district court. The Qui Tam suit is then forwarded to the Civil Division, DOJ by the local US Attorney. The suit is then generally sent through DoDIG to MPFU for preliminary investigation.

c. Qui Tam suits may be referred directly to a MPFU element by a local US Attorneys office.

d. Regardless of how a Qui Tam matter is received for investigation, the suit is filed under seal for 60 days. During this period investigative activity must be adequate to provide DOJ with sufficient credible data upon which to base a decision on whether or not to join in the suit.

11-12
Major procurement fraud investigation reports

MPFU investigative reports will be prepared in accordance with this regulation. Certain data elements common to all investigations involving contracts require additional report entries in initial and status reports.

a. Initial, status and SSI only reports: Reports will be prepared and submitted IAW Chapter 7 of this regulation. In addition, the following considerations should be addressed when preparing these reports:

(1) Report distribution: Copies of the reports should be provided to the MPFU element(s) in whose AOR either the victim procurement activity and/or subject contractor(s) are located. Copies should also be provided to the non-MPFU USACIDC elements if the investigation involves an installation within that unit’s AOR.

(2) Listing contractors as subjects: Care should be taken to use the full legal corporate or business name for all contractors or other businesses listed as subjects. Abbreviated or acronym corporate titles may be reflected in parenthesis after the full name.

(3) Supplemental information: MPFU supplemental data entries will be updated for each status or SSI report. Six elements of supplemental data are required following the status update:

(a) Other agent(s) and agency report numbers: List the full names of the case agents of other agencies participating in a joint investigation along with the case numbers of the other agencies' case actions. The lead agency should be identified.

(b) Impact: This section will include as complete a statement as possible of the adverse impact on the Army, including actual identified monetary damages, potential future monetary impact and all possible operational and safety consequences of the fraud.

(c) AUSA/SJA coordination: Provide the full names and titles of the AUSA and SJA attorney(s) briefed or coordinated with on the matter including the most recent dates of coordination, and the results of the coordination especially regarding acceptance or declination for prosecution.

(d) PFA/PFD coordination: Provide the full names and titles of the PFA(s) and PFD, OTJAG attorney(s) briefed or coordinated with on the matter including the most recent dates of coordination.

(e) Potential remedies: All potential remedies (criminal, civil, contractual or administrative) will be outlined.

(f) Potential return to the Army: This paragraph will list the areas, using the actual remedies process, where efforts will be made to achieve an actual return or specific benefit to the Army.

(4) Frequency of status reports: Status reports will be submitted IAW Chapter 7 of this regulation.

b. Interim reports: Interim reports will be submitted IAW Chapter 7 of this regulation. When they are submitted, distribution will include Director, MPFU, ATTN: CISAM-OP.

c. Final reports: ROIs will remain in an open status until all criminal prosecutions, civil prosecutions, contractual and/or administrative action(s) have been reported. When completed, final reports will be submitted IAW Chapter 7 of this regulation.

11-13
U.S. Attorney case presentations

a. MPFU investigative efforts are generally presented through the U.S. Attorney system for prosecution. The format and content for these presentations vary among judicial districts.

b. MPFU elements, at the time of formal presentation, will also present to the U.S. Attorney a formal summary of the presentation in one of the following formats:

(1) A prosecution presentation report under unit letterhead. Format and content will be determined by the special agent-in-charge.

(2) Agent’s investigation report (AIR), with attachments as required.

(3) Interim ROI as produced by the ACIRS system.

(4) In the written format and with the content as prescribed by the recipient of the presentation (local practice).

CHAPTER 12

12-1
Definitions

a. Army Computer Emergency Response Team (ACERT): A Land Information Warfare Activity (LIWA) component that assists Army network administrators in the identification and elimination of computer system and network vulnerabilities.

b. Army Network Operations and Security Center (ANOSC): Provides Army and DoD decision makers a comprehensive, integrated, near real-time, situational awareness and operational reporting capability of the Army's networks, critical systems, and designated applications that comprise the Army's portion of the global information grid.

c. Computer crime: A criminal act in which a computer is the target of the offense or is the tool by which the offense is committed or attempted. To avoid confusion, it is important to differentiate between a computer crime and instances when a computer is a mere storage device for evidence of a crime. In the first instance, the computer is either the target (victim) or the tool (instrumentality) of the offense. In the second instance, the involvement is incidental to the offense, but important to law enforcement because it contains evidence of a crime. For the purpose of this regulation, incidental involvement of a computer will be referred to as “incidental computer usage.” The term “computer” may refer to any device in which electronic data is created, edited, transmitted and/or stored (e.g., cellular phone, pager, electrical organizer, etc).

d. Computer Crime Coordinator (CCC): USACIDC personnel in each group, battalion and field office, normally assigned, as an additional duty, to coordinate computer crime investigations for their units, perform limited electronic media analysis, and to assist with or assume responsibility for computer investigations within their area of responsibility (AOR) where needed and when within their respective capabilities.

e. Computer Crime Investigations Committee (CCIC): An internal USACIDC forum designed as a coordination resource dealing with computer crime related procedures, standards, equipment, policies, and training issues. The CCIC is comprised of selected personnel from HQUSACIDC, CCIU, USACIL, and personnel designated as CCCs throughout USACIDC.

f. Computer Crime Investigative Unit (CCIU): A USACIDC investigative element created to provide direct Army law enforcement support to the Army Information Assurance program by conducting criminal investigations into suspected computer intrusions, select computer crime offenses and performing vulnerability assessments.

g. Computer incident: Any uncategorized computer anomaly or activity on a network not amounting to an intrusion or an attempted intrusion.

h. Computer intrusion: A computer crime characterized by the act of gaining intentional, unauthorized access to a protected computer or exceeding an authorized level of access, under the circumstances set out in 18 USC § 1030 (Fraud and Related Activities in Connection with Computers). For purposes of this regulation, intrusions include the offenses listed under the 18 USC § 1030(5) damage provisions, such as sending viruses, denial of service attacks, etc.

i. Computer Investigations: Computer investigations include the investigation of computer crime, as defined above, and incidental computer usage, in which computer evidence plays a role in the investigation. A computer investigation typically consists of four processes:

(1) search and seizure;

(2) examination of the system and creation of a forensic duplicate (image) of the original electronic evidence, to include restored data in a form appropriate for the investigator's use;

(3) review and analysis of the restored evidence; and

(4) preparation for criminal, civil or administrative action.

j. Computer Network Defense Operations Chiefs Working Group (CND OCWG): A Department of Defense (DoD) initiated coordinating group comprised of members from each Defense Criminal Investigations Organization (DCIO) and the Office of the Chief of Staff for Intelligence (ODCSINT). The CND OCWG is primarily chartered to develop planning, guidance, strategy, and policies to implement law enforcement, counterintelligence, forensics, and training support to DoD computer network defense across service/agency boundaries.

k. Electronic Crime Vulnerability Assessment (E-Crime VA): A formally recorded review and analysis, in support of the Army's Information Assurance program, of existing computer network security measures within a specified facility or activity. The E-Crime VA purpose is the detection of conditions or procedures conducive to criminal activity and minimizing or eliminating the opportunity to commit a criminal offense or gain unauthorized access into a protected computer network. E-Crime VAs will be scheduled, performed, documented, and managed IAW the provisions of chapter 10 of this regulation (Figure 1).

l. Defense Computer Forensics Laboratory (DCFL): The DoD laboratory established to process, analyze and conduct forensic examinations of electronic evidence in support of counterintelligence and criminal investigations.

m. Defense Computer Investigation Training Program (DCITP): The DoD agency responsible for proving computer crime and forensics training to DoD personnel.

n. Joint Task Force - Computer Network Operations (JTF-CNO): A DoD activity tasked with coordinating and directing the defense of DoD computer networks, under the authority and direction of the Secretary of Defense in conjunction with the unified commands, Services, and agencies. This mission includes the coordination of DoD defensive actions with non-DoD government agencies and appropriate private organizations through the National Infrastructure Protection Center (NIPC).

o. Incidental computer usage: The act of using electronic storage media, either permanent or removable, to store evidence of a criminal offense, e.g., e-mail, images, documents, and applications.

p. Information Assurance: An Army program that encompasses the Army's efforts to protect the confidentiality, integrity, and availability of data and systems.

q. Inter-Agency Coordination Cell (IACC): A subordinate element of the NIPC’s Computer Investigations and Operations Section, responsible for coordination and de-conflicting investigative efforts by agencies involved in the investigation of computer crime.

r. Land Information Warfare Activity (LIWA): The Army activity charged, in part, with ensuring the protection of Army interest computer systems and networks.

s. Local Computer Incident Response Team (LCIRT): Locally comprised information technology experts responsible for network security at the MACOM level or lower.

t. National Infrastructure Protection Center (NIPC): Created by Presidential Decision Directive 63, 22 May 98, the NIPC is the federal focal point for protecting against threats directed at the nation’s critical infrastructure, including cyber systems.

u. Protected computer: Any computer which:

(1) is used in interstate or foreign commerce or communication,

(2) used exclusively by a financial institution or the United States Government,

(3) or in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government when the conduct constituting the offense affects that use by or for the financial institution or the Government.

v. Regional Computer Emergency Response Team (RCERT): ACERT component that perform duties for a limited geographical area.

w. Theater Network Operations Security Center (TNOSC): The center of excellence for tactical through strategic networks providing integrated systems and security management serving as the operation proponent for information systems and Army domain management.

12-2
General responsibilities

a. The USACIDC is responsible for investigating intrusions and computer crime when association with a crime normally investigated by USACIDC IAW AR 195-2.

(1) The Deputy Chief of Staff for Operations (DCSOPS), HQUSACIDC, will establish and manage the USACIDC's Computer Crime Investigation Committee and appoint the committee’s chairperson . The committee will consist of selected personnel from the DCSOPS, the Deputy Chief of Staff for Information Management (DCSIM); the CCIU, the U.S. Army Criminal Investigation Laboratory’s (USACIL) Computer Forensics and Investigation Section, and others as appropriate. The DCSOPS will also appoint personnel to serve as members of the CND OCWG, the Law Enforcement and Counterintelligence Center (LECIC), JTF-CNO and the NIPC’s IACC.

(2) Each group, battalion, and field office commander will appoint, train and equip selected personnel as CCCs to meet the requirements of this regulation.

(3) The USACIL will provide advice and assistance on proper computer evidence procedures throughout the USACIDC and recommend changes in standards, policies, procedures, equipment needs, and training requirements, as warranted by developments in technology and the capabilities of those committing computer crime. USACIL has primary responsibility for coordinating computer forensic evidence issues with DoD organizations and other federal agencies. The Computer Forensics and Investigations section is responsible for conducting forensic examinations of computer media in support of USACIDC units when such support is not provided by CCCs. Additionally, the section will provide assistance in coordinating cases to be supported by the DCFL.

(4) The CCIU has primary responsibility for investigating computer intrusions and selected computer crime. Additionally, in matters that relate to Information Assurance and computer crime, the CCIU conducts liaison with DoD organizations and other federal agencies. In this capacity, CCIU recommends to the DCSOPS changes in standards, policies, procedures, equipment needs and

training requirements, as warranted by developments in technology that enhance the commission of computer crime.

(5) The Plans and Training Division has primary responsibility for the identification and facilitation of computer crime and electronic media analysis training throughout the command.

(6) Designated CCCs are responsible for the coordination of technical and investigative needs and the analysis of certain electronic storage media in support of their respective AOR's computer crime investigations. CCCs are also responsible for conducting liaison with local computer crime investigative agencies, providing computer crime training and recommending changes in standards, policies, procedures, equipment needs and training requirements as warranted by developments in technology and the capabilities of those committing computer crime.

b. The USACIDC and U.S. Army Intelligence and Security Command (INSCOM) each have certain responsibilities for the investigation of computer crime involving Army interest computers and computer systems.

(1) INSCOM is responsible for counterintelligence investigations of computer crimes that involve a foreign intelligence service (FIS).

(2) When credible information indicates a computer crime involves a FIS, the USACIDC and INSCOM will conduct parallel investigations as described in paragraph 12-6 below.

12.3
Computer Crime Investigations Committee (CCIC)

a. Scope. The USACIDC CCIC is a coordinating element focused on the functional specialties of computer crime investigations and computer media analysis.

b. Program objective. The objective of the CCIC is to optimize the criminal investigative posture of USACIDC by providing USACIDC investigators recommendations on state-of-the-art electronic investigative equipment, techniques and software, in accordance with CIDR 70-1 (Evaluation and Acquisition of USACIDC Equipment), Army supply regulations, and current industry standards. This committee will establish USACIDC requirements for such investigative equipment, techniques and software as outlined in this chapter. Communication between committee members will primarily take place through the command's Intranet site at:

http://160.147.87.16/intranet/ccc/computer crimes.htm

c. Responsibilities:

(1) HQUSACIDC

(a) CCIC:

1. Recommends USACIDC requirements for investigative equipment (hardware and software) and forensic techniques used during media analysis.

2. Identifies investigative equipment and techniques to be evaluated by USACIL, the CCIU and CCCs as appropriate.

3. Surfaces computer crime issues which need to be staffed, and directs such issues to the appropriate HQUSACIDC staff office and CCIC members as part of policy development and implementation.

(b) The ADCSOPS:

1. Serves as the primary HQUSACIDC action officer for computer crime matters.

2. Chairs the USACIDC CCIC.

(c) The HQUSACIDC Computer Crime Program Manager:

1. Reviews, when appropriate, computer crime reports to assure standards established by this regulation are complied with.

2. Manages and maintains the CCIC Intranet web site.

3. Acts as liaison between the CCIC and other USACIDC elements involved in the conduct of computer crime investigations and media analysis.

4. Along with the Plans and Training Division, determines and evaluates new training opportunities in the field of computer crime and electronic media analysis and recommends to the DCSOPS needed changes in USACIDC computer crime training needs.

(d) The Plans and Training Division: Determines and evaluates available computer crime and electronic media analysis training available throughout the DoD and other recognized training resources. In concert with the Computer Crime Program Manager, recommends adjustments to USACIDC training policies to meet new training needs and facilitates training opportunities throughout USACIDC.

(e) The DCSSPT: Provides guidance concerning the acquisition of computer equipment and software and serves as proponent for CIDR 70-1.

(f) Comptroller: Ensures that a level of funding commensurate with HQDA Program Budget Guidance (PBG) has been identified in the Command Budget Estimate (CBE) and the MACOM Program Objective Memorandum (POM) and is allocated during the fiscal year of execution to support the command Computer Crime program.

(g) DCSIM:

1. Serves as the primary HQUSACIDC action officer for information management.

2. Coordinates the acquisition of information equipment used in law enforcement.

3. Stays current in information technology through review of professional literature, self-study, and continuing education.

4. Provides a representative to the CCIC.

(h) USACIDC group commanders: Ensure computer crime investigative equipment, software and training needs are identified and met IAW this chapter and CIDR 70-1, as appropriate.

(i) Battalion, district and field office commanders will:

1. Identify needs for computer crime investigative equipment, software, and training.

2. Appoint a CCC for the unit.

(j) CCCs will:

1. Assist in the identification and evaluation of computer crime investigative equipment, techniques and software as requested by the CCIC IAW CIDR 70-1.

2. Ensure investigative equipment, techniques and software needs are identified to their chain of command.

3. Represent their unit commander on the USACIDC CCIC.

12-4
Specific USACIDC responsibility

a. The USACIL will:

(1) Provide USACIDC investigators and management with expert advice and assistance in all phases of computer investigations, to include laboratory and crime scene assistance when such advice and assistance is not available from the supporting CCC. Assistance includes, but is not limited to the following:

(a) Providing technical guidance and on scene assistance to USACIDC personnel regarding the preparation of search and seizure documents, seizure of computer equipment, and shipment of storage media devices for analysis.

(b) Examining computer systems and providing an evaluation of the technical aspects of the system.

(c) Duplicating stored data in a forensically sound manner while preserving the integrity of the original evidence.

(d) Recovering/restoring data and providing that data in a form that allows the SA to continue the investigation. This includes recovery of data from damaged devices and data that has been encrypted, password protected or deleted and includes determining information such as date created, modified, accessed, recovered, etc.

(e) Working, when necessary, with the agent on site or in the laboratory to assist in the investigation.

(f) Preparing forensic analysis reports of significant findings and conclusions and providing a presentation of the evidence.

(g) Providing authorized assistance, including to defense counsel under discovery rules, prior to and during criminal, civil, or administrative hearings.

(h) Providing testimony during criminal, civil, or administrative hearings.

(2) Perform the service enumerated above in support of requests for USACIL assistance by other Defense Criminal Investigative Organizations (DCIOs).

(3) Determine when computer evidence will be forwarded to another computer forensic facility, such as the DCFL, for examination and monitor the status of such laboratory support if the evidence is sent through USACIL.

(4) Represent USACIDC on appropriate committees formulating proposals for computer forensic and investigative policies, training, equipment and procedures.

(5) Through the CCIC, keep the DCSOPS updated on changes in computer forensic and investigative policies, training and procedures developed through liaison and participation in other computer crime related forums.

(6) Serve as the USACIDC subject matter expert to the CCIC on the physical seizure of computer media, packaging, and forensic analysis.

b. The CCIU will:

(1) Investigate allegations of computer intrusions, attempted intrusions or other selected computer crime.

(2) Provide direct law enforcement support to the Army Information Assurance mission by performing vulnerability assessments.

(3) Serve as USACIDC LNO for the following activities:

a. ANOSC,

b. CONUS-RCERT,

c. ACERT,

d. LIWA

e. TNOSC, and

(4) Provide a legal advisor with expertise in Information Assurance and computer technology to act as the primary legal advisor for USACIDC on computer crime legal issues.

(5) Collect, collate, and disseminate criminal intelligence on computer crime related issues.

(6) Develop and maintain network, media and system analysis capabilities to support computer intrusion investigations.

(7) Provide limited media and system analysis support to USACIDC units on a case-by-case basis. This support can include:

(a) Technical guidance to USACIDC SAs and CCCs on the preparation of search and seizure documents, seizure of automation equipment, and shipment of storage media devices for analysis.

(b) Recovery of files, when possible, and determination of information such as date created, modified, accessed, erased, etc.

(c) Reconstruction, when possible, of fragmented and/or deleted files.

(d) Preparation of reports of significant findings and conclusions as appropriate.

(e) Providing expert testimony during legal proceedings.

(8) Serve as the USACIDC subject matter expert to the CCIC on network intrusion investigations.

(9) Assist with research and development of electronic medium defense from intrusions as appropriate.

c. Designated CCCs will, upon completion of the training prescribed in paragraph 12-5 below, and within the limits of their AOR and available resources:

(1) Provide technical guidance to USACIDC SAs on the preparation of search and seizure documents, seizure of automation equipment, and shipment of storage media devices for analysis by DCFL, USACIL or CCIU when the analysis is beyond the technical capabilities, resources, or available time of the CCC.

(2) Duplicate, restore, and examine electronic storage media if the action is within the CCC's technical capabilities and resources.

(3) Reconstruct, when possible, fragmented and/or deleted files, records, and images, if the action is within the CCC's technical capabilities, resources, or available time.

(4) Prepare reports of significant findings and conclusions.

(5) Provide expert testimony during legal proceedings.

(6) Provide assistance to SAs as appropriate.

(7) Establish and maintain liaison with INSCOM counterparts.

(8) Establish and maintain liaison with RCERT/LCERT elements as appropriate.

d. USACIDC SAs will:

(1) Immediately coordinate all cases involving computer crime evidence with their CCC, the CCIU, or USACIL, as appropriate, to determine if crime scene support is required, and identify which activity will provide needed support.

(2) Prepare appropriate search and seizure requests.

(3) Seize computers, computer peripherals, and storage media as evidence.

(4) Determine need for computer investigation assistance and prepare seized evidence for shipment.

(5) Be prepared to respond immediately to a request for assistance (RFA) from the CCIU on a computer network intrusion.

12-5
Training

a. Due to the technical nature of computer crime investigations and investigations in which computers contain evidence related to offenses, specialized training is necessary so USACIDC SAs can successfully process a computer as evidence. Personnel attending the Apprentice Special Agent Course receive the Introduction to Computer Search and Seizure (ICSS) course as part of their initial training curriculum. Specialized training is available from a variety of sources such as the Federal Law Enforcement Training Center (FLETC) in Glynco, GA, the Defense Computer Investigation Training Program (DCITP) in Linthicum, MD, and various private commercial sources. In the absence of formal ICSS training, USACIDC units should make all efforts possible to ensure that unit-training programs include training on the proper procedures for seizing computer equipment as evidence. As resources are made available, all SAs should attend the listed below courses. The goal of USACIDC's training methodology is to have all SAs trained to the maximum extent possible in computer investigations. The DCSOPS may approve other courses and/or training sources as equivalent to the courses listed below:

(1) All USACIDC SAs should attend the following course to enhance their computer related investigative skills: Introduction to Computer Search and Seizure Course (DCITP).

(2) CCCs will attend the following courses in order to be considered fully qualified:

(a) Introduction to Computer Search and Seizure Course (DCITP),

(b) Introduction to Network and Computer Hardware Course (DCITP) or Criminal Investigations in an Automated Environment Course (FLETC),

(c) Basic Forensic Examinations Course (DCITP), or Seized Computer Evidence Recovery Specialist Course (FLETC), and

(d) Network Intrusion Analysis Course (DCITP) or Computer Network Investigations Course (FLETC).

12-6
Investigating computer network intrusions

a. Normally, the ACERT will notify the CCIU of all computer intrusions or incidents involving protected Army interest computers or computer systems. The affected system is considered a crime scene and the USACIDC must respond promptly. When the incident is outside the immediate geographical area of the CCIU, the CCIU may contact the appropriate USACIDC unit with a RFA to process the crime scene.

b. Upon notification of a computer intrusion or incident involving an Army interest computer or computer system, USACIDC will respond and conduct a preliminary investigation. If an INSCOM agent responds and a counterintelligence investigation is opened, CID will investigate the criminal aspects of the incident while the INSCOM element will conduct any required counterintelligence investigation involving the national security aspects of the incident. The USACIDC and INSCOM elements will conduct parallel investigations and will maintain close coordination with each other.

c. The processing checklist at figure 12-2 will be used in the conduct of any preliminary inquiry involving computer intrusions or incidents. If a SA assists the CCIU by conducting the preliminary investigation, the SA will complete and return the checklist electronically, or by facsimile machine, to the CCIU as soon as possible after notification of a computer intrusion. When an INSCOM agent is not available to respond, the CID case agent will, at the earliest opportunity, coordinate with the local INSCOM element and offer to provide a copy of the completed checklist.

d. The responding CID element will determine if classified information is involved and the level of classification. If applicable, classified information will be processed IAW Chapter 7 of this regulation.

e. When an active criminal investigation may have an adverse impact on an INSCOM counterintelligence investigation, the special agent-in-charge (SAC) of the responsible CID element may agree with the INSCOM element to hold the criminal investigation temporarily in abeyance pending further resolution of the national security interests. Should the SAC of the responding CID element believe the proposed INSCOM investigative actions would adversely impact the

resolution of the criminal investigation and an agreement cannot be reached, the matter will be referred to the chain of command for resolution.

12-7
Investigative activities

a. Investigative Reports: When a USACIDC element initiates an investigation regarding a computer crime, the initiation and conduct of the investigation will be documented in the report of investigation (ROI) format and IAW Chapter 7 of this regulation. Manpower data will be recorded in the responding CID field office's ROI and the offense code 9G2F (Other) used to identify the action as a computer investigation by SA, CCC, CCIU, or USACIL personnel. The same offense code will be used on preliminary investigations that do not result in an ROI.

b. Request for Assistance (RFA): The CCIU will occasionally dispatch a RFA requesting CID field offices to obtain and serve subpoenas and/or warrants on Internet service providers (ISP) or other similar activities. In support of these RFAs, the CCIU will provide the appropriate office with an affidavit in support of the warrant. These requests will be immediately coordinated with the supporting prosecutor and processed in an expeditious manner.

c. Computer investigation support and documentation:

(1) When a USACIDC unit requires computer investigation support from their CCC or the CCIU, such assistance will be in the form of a RFA. Documentation of such assistance will be provided to the supported CID field office in the form of an information report IAW Chapter 7 of this regulation.

(2) When computer investigation support from USACIL is required, the procedures in Chapter 26 of this regulation will be followed.

(3) When computer investigation support from DCFL is required, their request form will be used. This form will be made available, and updated as required, on the USACIDC web server and the DCFL site. As noted in Chapter 26 of this regulation, the Director, USACIL, must approve USACIDC personnel using a laboratory other than USACIL, if the needed services fall within the scope of the services provided by USACIL.

(4) Prior to forwarding electronic media for laboratory examination, coordination should first be made to ensure proper packaging and shipment procedures are employed. In addition, a copy of the search and seizure authorization must accompany the laboratory examination request to ensure that the scope of the search is not violated during forensic examinations.

d. Computer evidence: Information maintained on electronic storage media requires special handling to preserve the integrity of the evidence. Viewing files with non-forensic software, exposure to extreme elements, or loss of internal power will permanently damage or destroy the information stored in the device's memory. Details addressing the special handling requirements of electronic media are detailed in AR 195-5. In summary, personnel handling electronic media should take the following into consideration:

(1) Unless directed to do so by competent technical personnel, data stored on a computer should not be viewed using non-forensic software. Acts as insignificant as calling up a file will permanently alter evidence such as date and time stamps.

(2) Avoid exposing electronic media to adverse environmental conditions such as extreme temperatures, humidity or excessive dust and foreign materials. Exposure to such conditions will damage both the media and the data contained therein.

(3) Keep electronic media away from other electronic devices, batteries, telephones, microwaves, magnets, or materials that generate static. Exposure to any of these items will cause permanent damage to the data.

(4) When items are seized that require some sort of electrical power to function properly, periodically check these items to ensure that power is constantly available. In most cases, the loss of power to devices such as cellular phone, pagers, etc., will permanently erase all stored information.

e. Documentation and disposition of electronic evidence: Details addressing the special handling requirements for the disposition of electronic evidence are detailed in AR 195-5. In summary, personnel handling electronic media should take the following into consideration:

(1) At a minimum, copies of all evidence discovered during the course of a computer crime investigation must be permanently memorialized on new or sterilized media. IAW Chapter 7 of this regulation, a copy of such evidence will be attached to the final ROI as an attached exhibit.

(2) When a decision is made that the evidence discovered is sufficiently sensitive as to preclude its general dissemination (e.g. pornographic material), a copy of the evidence will be attached to the final ROI as an attached exhibit with limited distribution (i.e., CRC and file copies only).

(3) When the media used to copy electronic evidence allow for recycling (e.g., floppy disks, hard drives, tape, etc), coordination with the unit CCC must include appropriate steps to permanently remove any electronic trace of previously

recorded data through forensic processes such as wiping the disk of all data and residual remains (e.g., residual slack).

(4) Because of the uniqueness of electronic evidence, disposition of such evidence must be coordinated with legal authorities prior to permanent disposition to determine the legality of destroying the media or returning the media to its legal owner after the forensic removal of the contraband material.

12-8
Child Pornography, Adult Pornography and Other Obscene Matter

a. Title 18 USC, Sections 2251-2260, Sexual Exploitation and other Abuse of Children and Title 18 USC, Section 1460-1470, Obscenity, make it a federal offense to possess, distribute, import or transport (including by mail, common carrier or the use of a computer) what is commonly referred to as child and adult pornography (hereafter referred to as “prohibited images”). Child pornography is broadly defined as a visual depiction of a person under the age of eighteen engaging in sexually explicit conduct as defined in Title 18, section 2256.

b. As standard procedure, prohibited images found on a suspect computer are reproduced and restored to separate sterile media as either extracted evidence or as a “working copy” to be used during analysis. A MD5 hash value or a CRC Checksum of all extracted files will also be included on the media, as a method of authenticating the integrity of the images. To avoid storage of such images on numerous machines, and as allowed by resources, a single machine should be designated for use in media analysis and any subsequent viewing of images. When storage media is recycled (i.e., floppy diskette, hard disk, tape, etc), the media will be wiped (overwritten) with a government approved “wipe” utility or a wiping utility included with forensic software packages. When no longer needed, non-recyclable storage media (i.e., compact disks (CD), photographs, magazines, etc) will be physically destroyed.

c. Additional copies of prohibited images will be strictly limited and documented for in the AAS in the case file. The number of copies will be kept to a minimum. Case file documentation will ensure that every instance where such images are released is clearly documented in a memorandum for record (MFR) (Figure 12-3) and includes the name of the person to whom the images were provided and under what circumstances.

(1) Trial Counsel. When a trial counsel requests a copy of such prohibited images, the designated USACIDC case agent will comply with the request. In most cases, the images can be “burned” to a CD. The CD will be delivered to the trial counsel (i.e., JA or AUSA), either in person or through controlled mail (i.e., certified, registered, federal express, etc). The images will not be transmitted via e-mail or general distribution. The images will only be released to the trial

counsel with an accompanying MFR (Figure 12-3). These procedures also apply to “hard copy” images (e.g., photographs, magazines, etc). The MFR will be added to the case file for future reference.

(2) Medical Personnel. When working with a local pediatrician to determine the estimated age of those persons depicted in the prohibited images, the pediatrician should be asked to view the images at the USACIDC activity. If this is not possible, the procedures of c(1) above will be used. In addition to the MFR at Figure 12-3, written correspondence between the USACIDC element and the pediatrician will include instructions regarding legal prohibitions against possession of these images beyond that required to perform official duties. The case agent must advise the pediatrician not to make copies of any images, not to store any of the images on the computer used to view the images, and make clear that the provided images must be returned to the case agent along with the written medical opinion as to the age of those depicted. If a local pediatrician is not available or refuses to supply the evaluation of the child’s estimated age, then the evaluation should be requested through the Armed Forces Center for Child Protection, Department of Pediatrics, National Naval Medical Center, Building 1, Tenth Floor, 8901 Wisconsin Avenue, Bethesda, MD 20889-5600. The temporary release of the prohibited images will be documented on a MFR (Figure 12-3). Upon completion of the review, the doctor will return the prohibited matter and the MFR to the agent and the medical opinion. The MFR and the evidence media will be added to the case file for future reference.

(3) Defense Counsel. With the approval of trial counsel, defense counsel will be afforded the opportunity to view the prohibited images at the USACIDC activity. Requests for a copy of the images by defense counsel will be referred to the trial counsel under discovery rules. The USACIDC will not provide defense counsel with copies of such images, unless the request is approved by the trial counsel or ordered by the trial judge. Once approval is obtained for release to the defense counsel, the agent will control the prohibited images by releasing it on a MFR (Figure 12-3). The defense counsel will be advised that upon completion of the trial, the prohibited images must be returned to the agent for appropriate disposal. The MFR will be added to the case file for future reference.

(4) Attached Exhibits. Upon completion of an investigation, the case agent will attach a copy of the prohibited images or a CD of the prohibited images used to support the investigative conclusions to the USACRC copy of the report only (See Chapter 7, CIDR 195-1). Digital images will be contained in a CD and not published as hard copies. Copies of these images will not, under any circumstances, be maintained by the case agent or stored on any machine for historical or training purposes. In addition, prohibited images will not be attached to other copies of the final report, to include copies to the SJA, provost marshal, USACIDC intermediate elements, or concerned commanders. Final disposition of prohibited images retained in the evidence depository and investigative case file

will be in compliance with applicable guidance contained in paragraph b above, AR 195-5, and other procedures as applicable.

CHAPTER 13

13-1
Purpose

This chapter sets policies and procedures for the management of the USACIDC Drug Suppression Program. It explains both operational and administrative procedures for drug suppression activities. It is not intended to confer any rights, benefits, privileges or form of due process procedure upon individuals, associations, corporations or other persons or entities.

13-2
Responsibilities

a. The overall USACIDC Drug Suppression Program is under the direction of the Commanding General, USACIDC.

b. The office of the Deputy Chief of Staff for Operations, HQUSACIDC will:

(1) Implement and supervise the USACIDC Drug Suppression Program.

(2) Receive and analyze criminal intelligence reports concerning individuals suspected or identified as being involved in drug abuse or distribution, modus operandi, smuggling routes and identification of substances being abused by members of the Army. As appropriate, index and retain the aforementioned criminal intelligence reports.

(3) Monitor drug seizure statistical data and analyze significant trends of drug abuse within the Army.

(4) Receive and analyze sensitive and serious incident reports and final reports of investigation concerning drug-related incidents for command interest.

(5) Analyze crime prevention surveys of medical facilities and medical supply storage sites to detect evidence of pilferage or illegal diversion of drugs.

(6) Maintain effective coordination with other federal and DoD investigative agencies involved in the suppression of drug abuse.

(7) Identify drug suppression training requirements.

(8) Monitor and analyze all phases of the Drug Suppression Survey Program (DSSP).

(9) Develop, program, and monitor USACIDC participation in drug suppression training programs.

(10) Receive, process and coordinate requests for attendance at drug suppression training courses.

(11) Review drug suppression training curricula provided by the United States Army Military Police School to assure compliance with current policy and doctrine relating to the USACIDC Drug Suppression Program.

c. The office of the Deputy Chief of Staff for Support, HQUSACIDC, will:

(1) Coordinate with the Deputy Chief of Staff for Operations on the programming of selected personnel for drug suppression training.

(2) Coordinate with the Deputy Chief of Staff for Operations in making utilization assignments of drug suppression trained personnel.

d. All USACIDC major subordinate commands (except MPFU), battalion/field office commanders, and special agents-in-charge of resident agencies will:

(1) Organize and conduct an effective drug suppression program.

(2) Appoint a drug suppression coordinator and/or chief, drug suppression team to coordinate and conduct drug suppression activities within the organization's area of responsibility.

(3) Where feasible, establish level two drug suppression team (DST) in accordance with paragraph 13-7a of this chapter.

(4) Develop a standard operating procedure (SOP) to provide operational guidance in the conduct of drug suppression activities for special agent supervisors, special agents, MP and non- MP personnel assigned, attached, or detailed for duty with the DST (see figure 13-2).

(5) Continually evaluate the extent and scope of the illegal drug problem including sources, availability of drugs, use and delivery by Army personnel.

(6) Ensure the source program assists to develop and confirm information in suppressing drugs.

(7) Provide the appropriate level of training to all personnel assigned to DST duties.

(8) Provide overall supervision to members of the DST to ensure the team functions in accordance with this and other regulations; applicable federal, state, local, and host nation laws; and that operations are conducted in a safe manner.

(9) Maintain liaison with supported commanders and staff concerning drug suppression activities.

(10) Maintain liaison with appropriate levels of United States and host country law enforcement agencies on drug suppression activities within the limits of prevailing laws and agreements.

13-3
Policies

a. The USACIDC field elements will plan, organize, and execute an effective drug suppression program designed to assist supported commanders in reducing drug abuse within their commands.

b. The USACIDC field elements will coordinate their drug suppression program with appropriate staff officers of the supported command such as the provost marshal (PM), staff judge advocate (SJA) and alcohol and drug abuse officer to ensure that CID drug suppression activities are integrated into the supported command's overall Army Substance Abuse Program (ASAP).

c. The USACIDC field elements will develop procedures to enhance cooperation and coordination between CID and the PM regarding drug suppression teams. Drug teams composed of CID special agents, military police investigators (MPI), military police (MP), and non-MP personnel are the most effective means for combating drug abuse.

d. The USACIDC field elements will conduct off-post drug suppression operations only to the extent necessary to accomplish the unit objectives and only where there is a soldier targeted, or sufficient Army interest exists to justify a DoD Policy Memorandum Number 5 operation. Questions concerning Army interest in CONUS off-post drug suppression operations will be coordinated with the local installation commander through the staff judge advocate. Advance coordination will also be accompli shed with the appropriate civilian law enforcement agencies. The USACIDC policy for conducting off-post investigations will be the guiding factors for conducting these types of investigations.

e. Special agents selected for drug suppression duties and all personnel under the control of USACIDC for the purpose of performing drug suppression duties will be familiar with the contents of this chapter and will be thoroughly briefed by t heir supervisors on responsibilities, investigative procedures and conduct expected of them while performing their duties.

f. The USACIDC drug suppression operations in foreign countries will be conducted within the constraints of prevailing Status of Forces Agreements

(SOFA), diplomatic guidance, Army policies for such activities, applicable international agreements and United States law.

13-4
Objectives

The objectives of the USACIDC Drug Suppression Program are:

a. To detect distribution or smuggling of drugs destined for use by members of the Army, their family members, and DoD-affiliated civilians under Army investigative jurisdiction.

b. To interdict the flow of drugs and reduce their availability to members of the Army, their family members, other U.S. Forces members under Army investigative jurisdiction, and DoD-affiliated civilians under Army investigative jurisdiction.

c. To detect the possession, use, or distribution of drugs by members of the Army, their family members, or civilians affiliated with the DoD when their activities are under the investigative jurisdiction of the Army.

d. To assist, within the limits imposed by higher authority or federal law, federal, state, and local law enforcement agencies in identifying sources of drugs to members of the Army, their family members, and DoD-affiliated civilians under Army investigative jurisdiction.

e. To assist, as authorized by law and DoD policy, federal law enforcement agencies in the detection of international distribution or smuggling of drugs destined for the United States, its territories and possessions, in any circumstances where DoD property and DoD affiliated personnel are involved or a DoD interest exists.

13-5
General

Effective CID drug suppression operations require:

a. Extensive planning and coordination with supported commanders and staff offices.

b. Adequate number of drug suppression trained and highly motivated special agents, MPI, MP and non-MP personnel.

c. Effective use and supervision of sources.

d. Vigorous and continuous investigative activities.

e. Continuous analysis of criminal intelligence, drug related reports of investigation, MP reports and other drug abuse indicators such as medical and urinalysis reports.

f. Close supervision by team chiefs, special agents-in-charge, operations officers, and commanders.

13-6
Levels of drug suppression operations

The drug suppression program is organized into three levels.

a. Level One. Conducted only in overseas areas utilizing special agents in a covert role to identify high-volume, wholesale distributors supplying controlled substances destined for resale or use by DoD affiliated personnel.

b. Level Two. Conducted by special agents, MPI, MPs, and non-MP personnel, assigned or attached to local CID elements, who operate in a semi-covert capacity with the mission of identifying individuals distributing drugs to DoD affiliated personnel or near U.S. military installations.

c. Level Three. Conducted by special agents, MPI, MP, and non-MP personnel, assigned or attached to local CID elements, and individuals assigned by the local PM, who operate in an overt manner investigating reported or detected controlled substance violations by Army and DoD affiliated personnel.

13-7
Organization

a. Where feasible, each CID field office and resident agency will establish a Level Two DST, to ensure effective accomplishment of the USACIDC drug suppression program objectives outlined in paragraph 13-4. Resident agencies with a manning level of less than six special agents may designate the DST chief position as an additional duty; however, the appointed agent will provide the degree of supervision necessary to operate the drug team successfully.

b. A Level One DST will only be formed in overseas areas, where appropriate, and will operate under the control and supervision of a special agent-in-charge. The team will be formed under the provisions of AR 195-2.

c. A level Two DST will be formed under the provisions of this chapter; paragraphs 9-4 and 9-5; and AR 190-30, paragraph 3-14. Whenever possible, these teams should be formed jointly with the local supporting PM using CID, MPI/MP, as well as non-MP assets. When appropriate, law enforcement personnel of other military criminal investigative organizations (MCIO) may be members of the DST. Where such joint teams are formed, a memorandum of understanding (MOU) will be executed with the provost marshal or other involved agency. See appendix L for a suggested MOU guide. The DST will operate under the control of the local CID element. Where agreed upon, MPI/MP/non-MP assets may be attached on orders to the local CID element for a specified period, normally one year. The team chief of a DST will be the senior CID member of the team and will be responsible for the direct supervision of the team. Battalion/field office commanders, operations officers, and special agents-in-charge will oversee DST operations. Command of other than CID personnel not on orders assigning them to the CID element will remain with their respective unit commander.

13-8
DoD affiliation in CONUS and OCONUS

A person, group of persons, or organization is considered to be affiliated with DoD, whether within or outside the CONUS, its territories and possessions, if the individuals involved are:

a. Members of the Armed Forces on active duty or members of the National Guard and Reserve on active duty status.

b. Individuals residing on, having authorized official access to, operating any business, or operating as licensed vendors at any DoD installation or activity. This category includes family members of DA military and civilian personnel located OCONUS.

c. Employed by or contracting with DoD or any activity under the jurisdiction of DoD, whether on a full-time or consultative basis.

d. Individuals having authorized access to defense information.

e. Participants in other authorized DoD programs, including individuals upon whom investigations have been initiated under AR 604-20, AR 360-5, and DoD Regulation 5220.22R.

f. Individuals applying for any status described above, including individuals such as applicants for military service, pre-inductees, and prospective contractors.

13-9
Drug suppression operations within the territorial jurisdiction of the United States

a. Level Two and Three operations will be conducted according to the provisions of AR 195-2 and within the constraints found in AR 380-13 and the Posse Comitatus Act.

b. In accordance with AR 195-2, the USACIDC has primary responsibility for the investigation of drug offenses occurring on military installations, and may pursue drug offenses by military members in accordance with this and other regulatory guidance. On military installations, investigative actions for drug offenses committed by persons not subject to the UCMJ may, within the limits of existing law and regulations, include search, seizure, detention and other actions necessary to maintain good order and discipline on the installation. Notification of drug offenses involving civilians on military installations will be provided to the Drug Enforcement Administration (DEA) in accordance with the 1984 Memorandum of Understanding between the Departments of Defense and Justice, unless relief from this reporting requirement has been granted by the local U.S. attorney. Where concurrent federal and state jurisdiction exists, investigations may also be coordinated with state or local law enforcement agencies, as appropriate. If a civilian law enforcement agency chooses to exercise primary investigative jurisdiction, the investigation will, to the extent allowed by existing personnel resources, be conducted jointly with that agency. If the civilian agency controls the evidence seized in the investigation, the joint/final report of investigation (ROI) will reflect the substantiation the civilian agency used to indicate the substance seized was in fact a controlled/illegal drug. If a civilian criminal justice agency has chosen to decline investigative responsibility or not to pursue prosecution, that information will be documented in the report of investigation and brought to the attention of the supported commander and the supporting staff judge advocate.

c. Civilian law enforcement agencies are normally responsible for the investigation of drug offenses committed outside of a military installation. The USACIDC may undertake investigations of drug offenses off post under the following circumstances:

(1) Offenses by members of the Armed Forces may be investigated by the USACIDC to the extent authorized by the Manual for Courts-Martial and applicable laws and regulations. Prior coordination must be accomplished with appropriate local civilian law enforcement/prosecutorial authorities.

(2) Offenses by persons not subject to the UCMJ may be investigated by the USACIDC in accordance with the provisions of DoDIG Policy Memorandum Number 5, dated 1 Oct 1987.

d. All DST personnel will not conduct planned purchases of controlled substances from an individual not subject to the UCMJ, off the installation, without the local/civilian police being present. Prior to initiating an off-post drug operation , the DST will obtain concurrence to conduct the operation from the local/civilian police agency having jurisdiction for that geographical area. Further, the DST will coordinate with the supported civilian prosecutor's office and obtain a preliminary agreement to prosecute, if possible.

e. In those instances where a purchase is planned from an individual subject to the UCMJ, off the installation, the local/civilian police will be notified and requested to be present. In all cases where an apprehension is anticipated, the local police will be present.

13-10
Drug suppression operations outside the territorial jurisdiction of the United States

a. The USACIDC drug suppression operations (Levels One and Two) conducted outside the boundaries of United States military installations and facilities outside the territorial jurisdiction of the United States will be:

(1) Coordinated with and approved by the major U.S. Forces Commander being supported.

(2) Coordinated with the DEA attaché or the U.S. Embassy Narcotic Coordinators of the countries in which the drug suppression operations are to be conducted. In some cases the DEA attaché and the U.S. Embassy Narcotics Coordinator are the same person. (See AR 195-2, paragraph 3-33.)

(3) Coordinated with the federal, state, and local law enforcement agencies of the countries involved, as appropriate.

(4) Conducted in accordance with prevailing SOFA, other applicable international agreements and diplomatic restrictions.

(5) Conducted in accordance with 22 USC 2291(c)(1) which prohibits USACIDC members from apprehending or involuntarily restraining local nationals or participating with foreign police in any action which, under normal circumstances, would involve searches, the apprehension of or use of force against any person, unless such person is subject to Uniform Code of Military Justice (UCMJ) jurisdiction. This restriction does not:

(a) Apply on U.S. installations or facilities.

(b) Apply in emergency situations involving possible serious bodily harm.

(c) Apply when following off-post in immediate pursuit of persons suspected of committing offenses on-post.

(d) Preclude USACIDC participation in operations with civilian police who are apprehending non-military personnel, when U.S. military suspects are being apprehended concurrently for the same offense. The USACIDC participation must be limited to the apprehension of U.S. military personnel.

(e) Preclude USACIDC personnel from making on-scene identifications.

(f) Prohibit covert USACIDC personnel from consummating drug transactions to acquire criminal intelligence or evidence concerning drug distribution as long as force is not used or threatened except in self-defense.

(g) Apply to the activities of the U.S. Armed Forces in carrying out their responsibilities under applicable SOFA.

b. Level One, Two, and Three operations:

(1) Level One operations will be conducted only in overseas areas with special agents acting in a covert role. These operations are intended to identify high level traffickers of narcotics and dangerous drugs and to intercept control led substances destined for resale and/or use by U.S. Forces personnel.

(a) Level One operations are subject to any limits imposed by the major U.S. commander being supported.

(b) Level One drug suppression operations outside the Republic of Germany require the prior approval of the DoD General Counsel after review by the Office of the Army General Counsel, and by the Staff Judge Advocate, USACIDC. The major U.S. Commander must also approve all such Level One operations on a case- by-case basis and provide his approval to the USACIDC major subordinate commander before the USACIDC major subordinate commander seeks DA and DoD approval. Requests for approval will be sent to HQUSACIDC, ATTN: CIOP-CO-CN and CIJA-ZA in sufficient time to obtain proper authorization. Except in emergency situations, one calendar week is required to obtain such approval, after receipt of the request at HQUSACIDC. Emergency requests will be documented as such in the message request and will, in addition to the factors outlined in AR 195-2, paragraph 3-33, contain an explanation of the emergency nature of the request. The USACIDC SJA will review and forward the request to the Office of the Army General Counsel to obtain necessary DA and DoD approval.

(c) These prior approval requirements do not apply to those operations which have their origins within the boundaries of Germany but which then move outside of Germany during the course of the operation, as for example, continuing negotiations or finalizing a purchase.

(2) Level Two operations will be conducted by special agents, MPI, MP, and non-MP personnel assigned/attached to local CID elements and operating in a semi-covert capacity with the mission of identifying traffickers, wholesale or retail, who operate on or near military installations or areas where U.S. Forces personnel are stationed or frequent. Those persons identified as selling directly to U.S. Forces personnel may be targeted regardless of their proximity to the installations .

(3) Level Three operations will be conducted by special agents assigned to the local CID unit who operate in an overt manner investigating reported or detected controlled substance violations by Army and/or other DoD affiliated personnel. Level Three operations are also conducted by MP/MPI personnel assigned to the provost marshal or security officer.

(4) All levels of drug suppression operations will be conducted in accordance with AR 195-2.

13-11
Military Police drug suppression activities

a. AR 195-2 and AR 190-30 authorize the military police to investigate offenses involving use and possession of non-narcotic controlled substances, where the quantity involved is sufficient for personal use only, and there is no indication of distribution. However, USACIDC Level Two and Level Three operations may, as part of joint drug suppression operations, investigate simple use and possession of marihuana and dangerous drugs.

b. The quantity of non-narcotic controlled substances which would exceed that intended personal use is dependent upon the existing circumstances and must be determined on a case-by-case basis.

c. When MP investigate any drug-related offenses, they will do so according to AR 190-30 and must follow these required procedures:

(1) All offenses reported to or detected by MP which involve controlled substances must be reported to the nearest USACIDC unit without delay.

(2) The USACIDC must be provided the opportunity to interview subjects, suspects or witnesses in MP investigations involving non-narcotic controlled substances without having to assume control of the investigation. If USACIDC

assumes a MP drug investigation, the investigation will not be referred back to the MP.

(3) When assuming a controlled substance investigation, USACIDC may allow the MP to remain active in the investigation and to assist as necessary or appropriate.

(4) Any controlled substance acquired by the MP must be turned over to the MP evidence custodian or the appropriate USACIDC unit if a MP evidence room is not available. Although the USACIDC evidence custodian has full responsibility f or controlled substances turned over to CID, the MP must provide assistance in the packing, processing, and preparation of forms.

d. Found non-narcotic controlled substances may be referred to the MP for disposition according to AR 190-22.

e. Found narcotic controlled substances will be handled by the USACIDC DST or negotiated under the local MOU with the provost marshal to refer to the MP. Disposition will be made according to AR 195-5.

13-12
USACIDC procedures for monitoring MP drug suppression activities and/or assuming investigative jurisdiction

a. When a USACIDC element is notified by the MP that an investigation involving a controlled substance has been initiated, the USACIDC element will determine the following:

(1) If narcotics are involved, USACIDC will assume investigative responsibility. If non-narcotics, USACIDC will not normally assume investigative responsibility unless the quantity involved is beyond that amount established for personal use.

(2) If there is any indication of distribution by individuals involved in the investigation, regardless of the quantity of drugs involved, USACIDC will assume investigative responsibility.

(3) If continued investigation by the MP might compromise any ongoing investigation being conducted by CID or the utilization of a source by USACIDC or another investigative agency, USACIDC will instruct the MP to discontinue their investigation and USACIDC will assume investigative responsibility.

b. The USACIDC field element supervisor, normally the operations officer or special agent-in-charge will make the initial determination whether the MP or USACIDC will continue the investigation. This determination will be made after coordination with the MP desk sergeant or MP duty investigator and an

evaluation of the information received. Crime scene response by USACIDC will be on a case-by-case basis.

c. If the MP continue the investigation, a copy of DA Form 3975, Military Police Report (MPR), will be provided to the supporting USACIDC element. Information from the MPR will be entered in the criminal intelligence raw data file.

d. If a CID investigation is warranted, the duty or DST agent will assume investigative responsibility, conduct a preliminary investigation and prepare the necessary documentation. Documents prepared by the MP prior to USACIDC assumption will be obtained and included in the report.

13-13
Field test analysis of suspected controlled substances

a. Under no circumstances will controlled substances be field tested if such testing will hinder further testing at USACIL. The following guidelines will apply:

(1) Identifying characteristics such as logos, score lines, coatings, and dimensions should not be destroyed if only one dosage unit of an item exists.

(2) Field tests should not be performed on liquids, oils (except suspected liquid hashish), blotters, or residues found in paraphernalia.

b. The results of the field test and the type of field test used will be included in the narrative of the report of investigation. Use of CID Form 36, Field Test Analysis of Suspected Controlled Substances, as an exhibit to the report of investigation is an alternate method for reporting the results. A statement of a positive or negative reaction will be recorded on the CID Form 28, Agent Activity Summary, together with a brief description of the observed change, i.e., immediate light blue color, changing to dark blue color. This information, if applicable, should also appear on the DA Form 3655, Crime Laboratory Examination Request.

c. The action commander will be contacted to determine what course of action will be pursued against the suspected offender. The case agent will brief the commander that if non- judicial/administrative action will be pursued, and if the substance appears to be marihuana plant materials, the substance will only be field tested and the results furnished to him. The commander will also be told that unless the USACIDC element is notified within 45 days of any change in action or that court-martial action will be initiated, the evidence will be destroyed according to AR 195-5. The commander must clearly understand that:

(1) Color tests are never conclusive analysis.

(2) Laboratory analysis is required for judicial action against the illegal possession of any suspected controlled substance.

(3) Laboratory analysis is required for any punitive non-judicial/administrative action against the illegal possession of any suspected controlled substance, except marihuana plant material.

(4) Early notification to the CID element will preclude unnecessary delays in obtaining laboratory reports.

d. When the suspected offender is not subject to the UCMJ, a determination will be made with the supporting law enforcement agency to determine if criminal prosecution will be pursued. If no criminal prosecution will follow, field test results will suffice for CID reporting criteria.

e. All USACIDC elements will submit the following for USACIL analysis regardless of action to be taken by commanders:

(1) All suspected controlled substances except marihuana plant material, which will be submitted if judicial action is to be pursued.

(2) All other substances, controlled or not, which are suspected of being abused.

13-14
Investigation of deaths caused by drug overdose

a. Under the provisions of AR 195-2 and Chapter 5 of this regulation, USACIDC units will investigate deaths which result from the suspected use of controlled substances.

b. All USACIDC elements will coordinate with local medical and MP authorities to ensure prompt notification when a suspected drug connected fatality has occurred or is likely to occur.

c. Military or DoD-affiliated personnel receiving medical treatment for an actual or possible drug overdose are automatically referred to the ASAP by the attending physician. Evidence gathering and reporting processes will be initiate d only upon notification that medical prognosis indicates that death is likely to occur from the drug overdose.

13-15
DoD assistance in drug interdiction and suppression

a. Requests for DoD major resources, such as helicopters or special equipment, in support of drug interdiction by any foreign, federal, state or local agency must be channeled through the requesting agency's headquarters to their federal, state and local attorneys to the Department of Defense, ATTN: Deputy Assistant Secretary of Defense (Program Management), Washington, DC 20301. These instructions pertain to all DoD resources including manpower, buildings, and equipment, except emergency medical and evacuation services.

b. These instructions are not intended to restrict USACIDC and non-DoD agency drug investigations, but to ensure that requests for DoD support to non-DoD agencies in support of their own drug law enforcement effort are cleared by the Office o f the Secretary of Defense.

c. Any USACIDC personnel receiving requests for support are prohibited from making any commitment concerning the availability of the requested resources. Soliciting such requests is also prohibited. Personnel receiving other than routine requests should instruct the requester to follow the procedures outlined in paragraph a, above. Once the requester has been instructed on the procedure to obtain the desired support, the office originally receiving the request should notify the Commanding General, USACIDC, ATTN: CIOP-CO-CN, of the request. In emergency cases, during non-duty hours, telephonic requests will be made to the USACIDC staff duty officer and followed by a written request. Such requests must contain adequate information concerning the circumstances and any plan of action, in order for HQUSACIDC to make appropriate recommendations to HQDA.

d. Upon notification of a forthcoming request for support, the Office of the Deputy Chief of Staff for Operations, HQUSACIDC, will effect appropriate internal staff coordination and notify HQDA (DAMO-ODL) of the impending request in order that a timely response may be given when the request is received by DoD.

13-16
Army Substance Abuse Program (ASAP)

a. A USACIDC element will not investigate participants in the ASAP for controlled substance offenses based on a person's enrollment in the ASAP. Independent credible information must exist to conduct an investigation of a participant in ASAP.

b. Special agents will not approach ASAP participants for the purpose of soliciting information about controlled substance offenses unless the participant voluntarily offers to provide such information. If the participant volunteers, the in

formation will not be obtained in the local ASAP facilities or in such a manner as to compromise the credibility of the ASAP.

c. Special agents or other members of a USACIDC DST will not employ sources in ASAP facilities or approach ASAP participants for the purpose of soliciting information about controlled substances.

d. The provisions of AR 600-85, Army Substance Abuse Program, apply when individuals have been identified as a controlled substance abuser through urinalysis screening.

e. When it is brought to the attention of CID that an individual has been identified as a drug offender through urinalysis testing, the CID unit receiving notification will, IAW paragraph 4-41, initiate an ROI when appropriate and pursue the investigation as though the individual was found in actual possession of the controlled substance.

f. All USACIDC elements will coordinate with the supported commander to express the goals of the command and to receive information from the ASAP program on drug abuse problems of the command. All commanders are enjoined to support fully the ASAP and instruct personnel engaged in drug suppression operations to respect the spirit of the program.

13-17
Possession or distribution of controlled substances

a. Under no circumstances, even to facilitate investigative activity, will USACIDC personnel or personnel acting on behalf of USACIDC in drug suppression activities, engage in the illicit possession or distribution of controlled substances or direct that others do so.

b. Under no circumstance will USACIDC personnel or personnel assigned to drug suppression duties supply controlled substances to any source, suspect or subject for any purpose. The USACIDC's involvement in controlled postal deliveries of controlled substances is outlined in paragraph 13-22 of this chapter.

c. All controlled substances in the possession of USACIDC or DST personnel will be properly documented and accounted for according to AR 195-5 and this regulation.

13-18
Controlled purchases, confidence buys, and fronting

a. Controlled purchases or confidence buys of controlled substances are made with limitation .0015 contingency funds in accordance with AR 195-4. Funds will be referred to as "CID funds" in all USACIDC reports.

b. Controlled purchases by a source should be completed under the supervision of a special agent who will ensure that the source is not in possession of any controlled substances or money other than the CID funds provided for the purchase. To ensure the source is not in possession of any funds other than CID funds, or is not in possession of any controlled substances not obtained under the supervision of USACIDC, a strip search will be conducted before and after each operation, unless special circumstances preclude such searches. Sources engaged in the purchase of controlled substances under the supervision of USACIDC should be kept under continuous surveillance when at all possible, unless operational or special circumstances preclude such surveillance. The use of sources is governed by Chapter 14.

c. The fronting of .0015 funds is authorized for the purchase of illicit drugs when deemed appropriate. The approval level for fronting CID funds is the same as expenditure limits outlined in AR 195-4. Loss or theft of .0015 funds is covered in AR 195-4, paragraph 1-9.

d. Supervisors will ensure that any fronting operation incorporates the following:

(1) Credible and reliable information available and documented to support the necessity of the fronting.

(2) Precise plan to monitor and control its execution.

(3) Involvement of first line supervisors to closely control and monitor any fronting transaction from its approval until its conclusion.

(4) To the extent possible, continual surveillance will be maintained over the subject being fronted the CID funds.

(5) Limitations on the length of time a subject is allowed to retain funds in his possession.

(6) If off an installation and when targeting an individual not subject to the UCMJ, coordination with the appropriate civilian law enforcement agency.

e. Controlled substances obtained through controlled purchases, confidence buys or fronting will be processed in the same manner as other evidence.

13-19
Use of controlled substances by special agents and personnel performing drug investigation duties

a. Special agents and personnel performing drug suppression duties under USACIDC control will not knowingly consume, smoke, inject or in any other manner use an illegal controlled substance while in covert or semi-covert status except when:

(1) Under extreme conditions of physical duress and then only after all reasonable methods of excuse have been exhausted.

(2) To refuse to do so would cause serious bodily harm or injury or pose an immediate threat to the person's life.

b. Special agents and DST personnel may simulate the use of controlled substances under exceptional circumstances. Personnel assigned to drug investigation duties will not simulate the use of controlled substances except, when in the individual's judgment, failure to do so would jeopardize their covert status or place them in jeopardy of physical injury.

c. DST personnel will report to their supervisors as soon as possible the circumstances involving the use or simulation of controlled substances during undercover activities.

d. Sources will be instructed to report to their respective handlers any use or simulated use of any controlled substance as soon as possible after the occurrence.

e. The USACIDC battalion/field office commanders will review each situation where a special agent, DST member or a source under CID control either simulates or is compelled to use a controlled substance. If only simulation took place, the fact s and circumstances will be entered on a CID Form 28, Agent Activity Summary, and reviewed and approved by the battalion/field office commander. If deemed appropriate, the battalion/field office commander may direct the drug suppression team member to submit to urinalysis testing. If it is determined that use actually occurred, the facts and circumstances will be documented in a CID Form 94, Agent's Investigation Report (AIR), and reviewed by the battalion/field office commander, who, if satisfied the use was not willful, will close the matter and forward a memorandum stating his conclusion and a copy of the AIR through the USACIDC major subordinate commander to the Commander, USACIDC, ATTN: CIOP-COP-CN. If there is reason to believe the use was willful and not consummated under coercion or duress, an inquiry will be initiated as a sequence number action by the USACIDC major subordinate commander. Should subsequent investigation determine the act was willful, a report will be initiated for the appropriate offenses. When an inquiry has been

initiated as a sequence number action and it is later determined that the use was, in fact, due to coercion or duress, the inquiry will be completed and a copy of the results will be forwarded through the USACIDC major subordinate commander to Commander, USACIDC, ATTN: CIOP-COP-CN.

f. The USACIDC battalion/field office commanders will ensure special agents, MPI, MP, and non-MP personnel assigned to drug suppression operations are knowledgeable of the contents of paragraph 13-19.

13-20
Federal agencies involved in drug suppression activities

The war on drugs involves a myriad of federal, state, and local agencies, and the list grows on a daily basis. All personnel involved in drug suppression operations must strive to stay abreast of agencies involved, specifically those in their AOR.

13-21
Reports

a. Reports of investigation pertaining to drug offenses will be prepared according to this regulation.

b. Serious and sensitive incident (SSI) reports involving controlled substances will be submitted according to Chapter 7, and will reflect the weight and/or volume, as applicable, of the controlled substance in metric measurements or by number of units. Figure 13-1 is provided as a guide for measurement conversions in reporting controlled substance seizures.

c. The CID Form 97, Criminal Intelligence Report (CIR), submitted on drug suppression operations should give special attention to the following areas:

(1) Modus operandi of drug violators.

(2) Distribution routes directed toward U.S. Forces.

(3) Organized distribution impacting on U.S. Forces.

(4) Appearances of new drugs, methods of concealment, use, and pricing.

(5) Availability of controlled substances to U.S. Forces, to include non-DoD personnel involved in introducing controlled substances onto military installations when appropriate and not in violation of AR 380-13.

(6) Drug trend analysis based upon accumulated information.

d. All CIRs concerning apprehended or identified civilian drug traffickers not listed in an ROI will include the perceived level (i.e., low, medium, high) of distribution. That level of distribution and any substantiation of their involvement with U.S. Forces should be included in the synopsis of the report. Particular attention must be given to verifying/documenting the military connection and military interest in instances dealing with personnel not subject to the UCMJ.

13-22
APO First Class Mail controlled substance seizure investigations (CONUS)

a. The USACIDC investigates the distribution of controlled substances through the U.S. postal system for three purposes:

(1) To interdict the flow of controlled substances through the mail system.

(2) To identify DoD-affiliated drug violators abusing the mail system.

(3) To deter other potential drug violators from using the mail to distribute controlled substances.

b. Investigations of controlled substances seized from first class mail are accomplished in cooperation with the U.S. Postal Service (USPS), U.S. Customs Service (USCS), and the Drug Enforcement Administration (DEA).

c. A USACIDC element will conduct a preliminary inquiry and/or investigation, as appropriate, when a military or DoD affiliated person is identified as the sender or addressee of mail containing a controlled substance as defined in the Controlled Substances Act of 1970.

d. The identification of non-DoD affiliated personnel will be conducted according to DoD 4525.6M, DoD Postal Manual. Names of individuals involved in these investigations will be provided to the appropriate civilian law enforcement agencies for investigation.

e. All USACIDC personnel are not authorized to have possession of or to read mail that has not been voluntarily released by its owner against receipt, seized by a search warrant or obtained in accordance with procedures involving confinement facilities.

f. Responsibilities.

(1) A USACIDC element having APO mail ports of entry into the Customs Territory of the U.S. located in their area of responsibility will coordinate with USPS, USCS and DEA for the processing of these violations.

(2) A USACIDC element located in an overseas area will conduct investigations of those violations referred to them from USCS when the sender is identified as being located in their area.

(3) The HQUSACIDC will conduct national level coordination and liaison with interested federal agencies, facilitate the investigative process when appropriate, and monitor the overall effectiveness of these investigations.

g. Investigative procedures.

(1) The USCS completes a seizure report, USCS Form 151, on each seizure of contraband discovered in the APO mail and forwards a copy to DEA to determine their investigative interest. An information copy is also provided to the USACIDC unit.

(2) The USCS detains the mail and contraband for 10-30 days to allow time for DEA or another interested agency to assume investigative jurisdiction and obtain a search warrant for the detained items.

(3) The USACIDC element receiving the seizure report coordinates with DEA and other concerned federal agencies to determine their investigative interest. If one of these agencies initiates an investigation which involves DoD-affiliate d personnel, a criminal intelligence report will be prepared indicating the circumstances of the offense.

(4) The USACIDC will assume investigative jurisdiction within five working days when a DoD-affiliated person is suspected of the offense; DEA has declined investigative jurisdiction; and no investigative interest is shown by any other federal agency.

(a) A CID sequence number action will be initiated for all seizures obtained from USCS.

(b) An attempt will be made to identify the status of the sender by comparing the information on the USCS Form 151 with Army worldwide locator data available at the CRC and any other locator source which would assist the investigating USACIDC element in identifying the sender.

(c) For seizures of small quantities of marihuana/hashish and dangerous drugs, indicative of personal use only, if sufficient identifying data is not available, the action record folder will be so annotated and no further action taken.

(d) In situations where U.S. mail originating in the APO mail system contains controlled substances and the sender can be identified sufficiently to permit an investigation, the following steps will be taken:

1. A federal district court must issue a search warrant to seize the mail and contraband substances contained therein. The warrant must be issued to a federal officer, i.e., USCS, DEA, or USACIDC.

2. The local CID element receiving the information and evidence will forward a letter to the overseas USACIDC unit explaining that the evidence is being retained for later release to the controlling office. The letter will include a copy of the search warrant and supporting affidavit.

3. A copy of the letter will be retained in the originating office case file.

(e) The action record folder will be completed when the above procedures have been applied to all the seizures for that date.

(5) The overseas USACIDC element receiving the evidence will initiate a sequence number action and, if appropriate, a ROI. Upon completion of investigative and judicial actions, the evidence will be disposed of in the following manner:

(a) The contraband controlled substances will be destroyed in accordance with AR 195-5.

(b) The seized letter and envelope will be sent Registered Mail Return Receipt Requested (Postal Form 3811) to the original addressee on the seized letter. The seized letter will have enclosed a USACIDC letter addressed "To Whom it May Concern" stating that the letter was delayed as evidence in a criminal proceeding. When delivery can be accomplished, the seized letter will be returned by Postal Form 3811 to the sender. If this cannot be accomplished, then the seized letter will be disposed of in accordance with the provisions of AR 195-5 pertaining to unreturnable evidence.

13-23
Security of Army Post Office mail overseas (OCONUS)

a. Based on an agreement with the USPS, DoD assumes responsibility for the security of military post office (MPO) mail overseas.

(1) This policy permits DoD officials to inspect, search, and collect information concerning MPO mail overseas when consistent with the Fourth Amendment to the U.S. Constitution, the UCMJ and the Manual for Courts-Martial.

(2) This policy will not impact on current guidance indicated in paragraph 13-22, regarding APO programs operating within CONUS, but will greatly assist law

enforcement officials in stemming the flow of drugs and other contraband into and out of overseas areas.

b. Procedures pertaining to the search and seizure of APO mail overseas are outlined in DoD 4525.6M, DoD Postal Manual.

13-24
Seizure and forfeiture of vehicles

Pursuant to a lawful search, inventory or inspection, military investigative authorities (CID, MPI or MP) may seize vehicles reasonably believed to constitute evidence of a crime or which might be used to resist apprehension or for escape (see section VI).

13-25
General

The USACIDC Drug Suppression Survey Program (DSSP) is a statistical review and analysis of drug suppression efforts and identifies projected trends for the future. The assessment quantifies the level of drug-related crime within the area of responsibility of the CID element based upon the analysis of the demand, reduction results from the CID drug suppression team(s), actions taken against drug violators, and results of the Army Substance Abuse Program (ASAP).

13-26
Objectives

a. A DSSP prepared by a CID field element is to provide the supported installation/community commander with reliable information upon which to base drug suppression goals and resource management decisions.

b. A DSSP prepared by HQUSACIDC is to provide senior Army leadership and subordinate elements with reliable information upon which to base drug suppression goals and resource management decisions.

13-27
Field Element Responsibilities

a. Determine annually whether a DSSP is needed. A decision to not conduct a DSSP must have the concurrence of the operations officer of the next higher headquarters (i.e., district/battalion or field office). The determination should be based on the amount of illegal drug activity/criminal intelligence in the area of

responsibility, and other factors to determine whether a DSSP is appropriate and beneficial to commander(s). A decision to not prepare a DSSP will be coordinated with the supported installation provost marshal/DOD police chief and command group. If differences of opinion exists as to the need to conduct a DSSP, the matter will be raised to the next higher CID headquarters for resolution.

b. Ensure that installation/community commanders within their area of responsibility are informed of the conduct and results of the DSSP. Copies of the DSSP assessment will be provided to the installation/community commander and the supported provost marshal/DoD police chief.

c. Ensure that drug suppression activity is conducted within their area of responsibility commensurate with the findings and recommendations of the DSSP report, and availability of investigative resources.

13-28
Execution

A field element conducting an assessment of its area of responsibility may combine branch office information.

13-29
Reporting format

The USACIDC field elements will prepare the DSSP report in a manner best suited to support the respective installation/community commander.

13-30
Reporting requirements

a. When a DSSP report is deemed appropriate it will encompass one complete calendar year from 1 January through 31 December in the event that a higher headquarters wants to consolidate information from subordinate offices.

b. The DSSP report will be distributed as follows:

(1) The original to the supported installation/community commander.

(2) One copy to the supported provost marshal/DOD police chief.

(3) One copy to the next higher headquarters (district/battalion or field office). The next higher headquarters has responsibility for reviewing the report for significant information that should be further reported to the USACIDC major subordinate command and HQUSACIDC, ATTN: CIOP-COP-CO as deemed appropriate.

(4) One file copy.

13-31
Coordination

Continuous coordination with other federal agencies is essential for an effective drug suppression program. The CID interfaces regularly with those other federal, state, local and foreign agencies, as required, to expedite the successful completion of investigative operations or exchange information with the agency having primary investigative and prosecutive jurisdiction. For a better understanding of the role various federal agencies perform in drug-related matters, a summary of their respective missions and responsibilities is provided. The majority of these agencies do not have missions which directly affect U.S. Forces in foreign countries.

13-32
Responsibilities of federal agencies in drug suppression activities

a. Federal Bureau of Investigation (FBI). The FBI is the primary federal law enforcement agency charged with enforcement of the criminal code of the United States. In addition, the FBI has concurrent jurisdiction with the DEA regarding the enforcement of drug laws. The Director, FBI, has overall responsibility for the direction, coordination, and management of drug enforcement activities within the U.S. Government and reports directly to the Attorney General of the United States.

b. Drug Enforcement Administration (DEA).

(1) The DEA is the primary arm of the U.S. Government charged with enforcement of U.S. controlled substance laws. The Administrator, DEA, reports directly to the Director, FBI, on drug matters. Domestically, DEA works closely with the FBI on high level drug investigations. The DEA's relationship with the CID overseas involves essentially the exchange of international drug trafficking information.

(2) In 1985, USACIDC and DEA joined an agreement wherein drug related intelligence meeting an established criteria would routinely be reported to the El Paso Intelligence Center (EPIC), El Paso, TX. Initial/SSI and subsequent status

report messages meeting one or more of the criteria below will be prepared listing LNO USACIDC-EPIC LNO FT BLISS TX //CIRFB-LNO// as an information addressee. Criminal Intelligence Reports (CIRs) containing information meeting the reporting requirements will be submitted via electrical message or electronic mail, again listing the Fort Bliss USACIDC-EPIC-LNO as the addressee and an information copy addressed to CDR HQUSACIDC WASH DC //CIOP-IN. The DEA - CID agreement also allows for queries from the field of EPIC's database. Requests of this nature must be routed through the respective USACIDC major subordinate command drug coordinator to EPIC. The EPIC will not honor direct queries from the field as access is limited to the USACIDC major subordinate command drug coordinators and designated USACIDC command staff. The following is the EPIC reporting criteria for Initial/SSI/CIRs:

(a) 23 kilograms or more of marihuana.

(b) 250 grams or more of methamphetamine.

(c) 453.59 grams or more of cocaine.

(d) 100 grams or more of heroin.

(e) 2,000 dosage units or more of, or 197 grams of, ephedrine/pseudoephedrine

(f) 2,000 dosage units or more of ecstasy, prescription controlled substances, steroids or any other dangerous drugs

(3) U.S. Customs Service (USCS). The USCS has the responsibility of interdicting and seizing contraband, including illegal drugs, entering the United States. Their interdiction of contraband entering the United States through the APO mail system and shipments of household goods has assisted the Army in identifying drug violators.

(4) U.S. Department of State. The State Department maintains liaison with U.S. and foreign law enforcement and intelligence agencies and leads the Cabinet Committee on International Control of Narcotics. The Department of State coordinates all narcotics suppression activities by federal agencies to include USACIDC outside of the United States.

(5) Defense Intelligence Agency (DIA). The DIA receives, correlates and exchanges drug information received and reported by the U.S. military intelligence agencies. The exchange of drug-related intelligence collected by military intelligence agencies within DoD is accomplished by DIA.

(6) Immigration and Naturalization Service (INS). The INS has the responsibility of denying U.S. passports or visas to identified drug traffickers and

of deporting those foreign nationals in the U.S. involved in illegal drug trafficking or production. The INS provides limited support to the suppression of drug abuse among U.S. Forces overseas.

(7) U.S. Postal Service (USPS). The mission of the USPS is to protect the U.S. mail and mail system, to include the investigation of the illegal transmission of narcotics and other controlled substances through the U.S. mail or sending any information facilitating the transfer of narcotics through the mail.

13-33
Guidance

Guidance on the scope of drug investigative activities and implementation of DoD Directive 5525.7 (Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense relating to the Investigation and Prosecution of Certain Crimes, January 22, 1985), as it relates to drug investigations.

a. "Appropriate prosecutorial authority" means:

(1) A United States attorney;

(2) A federal civilian investigative organization designated by the U.S. attorney to receive information concerning a particular case or class of cases;

(3) A prosecuting attorney of a local jurisdiction when the U.S. attorney has declined to exercise jurisdiction over a particular case or class of cases;

(4) An investigative organization designated by a prosecuting attorney of a local jurisdiction to receive information concerning a particular case or class of cases reference subparagraph 13-33a(3) above.

b. "Military installation" includes an aircraft, vessel, or other facility under military control.

c. "DoD personnel" means civilian employees of the Department of Defense and members of the Armed Forces.

d. "Immediate source" means a person who is directly and immediately involved in the transfer or distribution of illegal drugs to DoD personnel.

13-34
Policy

a. General. Drug offenses by DoD personnel and the introduction of drugs onto military installations adversely affect the efficiency and effectiveness of DoD programs.

b. Investigative actions on military installations. Military criminal investigative organizations have the primary responsibility for investigating drug offenses on military installations under DoD Directive 5525.7. The investigation of drug offenses on military installations, committed by persons not subject to the UCMJ, may include, on the installation, search, seizure, detention of persons, and other actions necessary to maintain good order and discipline on the installation to the extent authorized by the Secretary of the Army.

c. Investigative actions outside military installations. The investigation of drug offenses outside the military installation normally is the responsibility of non-DoD law enforcement officials. The following investigative actions outside military installations are authorized and may be conducted under regulations prescribed by the Secretary of the Army, subject to the requirements set forth below:

(1) Investigative actions involving members of the Armed Forces. Drug offenses by members of the Armed Forces may be investigated by USACIDC to the extent authorized by the Manual for Courts-Martial, DoD Directive 5525.7, rules issued by the Secretary of the Army, and other applicable laws and regulations.

(2) Investigative actions involving persons not subject to the Uniform Code of Military Justice. The USACIDC may undertake investigative actions with respect to a person not subject to the UCMJ:

(a) If there are reasonable grounds to believe that such person has committed a drug offense in conjunction with a member of the Armed Forces, and the investigative actions are undertaken to obtain evidence concerning all illegal drug transactions between such a person and any member of the Armed Forces.

(b) If there are reasonable grounds to believe that such person is the immediate source of the introduction of illegal drugs onto the military installations and the investigative actions are undertaken to obtain evidence concerning all persons engaged in drug trafficking on the installation.

d. Investigative policies. In conducting investigations outside the military installation under this subsection, the following policies apply:

(1) All investigations will be coordinated with the appropriate prosecutorial authority.

(2) DoD personnel assigned to or under the control of military criminal investigative organizations may be utilized as informants and undercover agents for the purposes set forth in this paragraph. They may obtain evidence concerning illegal drug transactions by military personnel or other persons engaged in illegal drug trafficking on the military installation.

(3) The USACIDC may participate in joint investigations with non-DoD law enforcement organizations for the purposes set forth in this paragraph. Those organizations may obtain evidence concerning illegal drug transactions by military personnel or other persons engaged in illegal drug trafficking on the military installation.

(4) Purchases of illegal drugs from persons not subject to the UCMJ may be made outside military installations for the purposes set forth in this paragraph. Those organizations may obtain evidence concerning illegal drug transactions by military personnel or other persons engaged in illegal drug trafficking on the military installation.

(5) Unless otherwise authorized by law, personnel assigned to the USACIDC may not participate in searches, arrests or apprehensions of persons not subject to the UCMJ. Such personnel may, however, be detained on military installations by CID special agents until they can be released to appropriate civilian law enforcement authorities. Personnel assigned to the military criminal investigative organizations may provide information to non-DoD law enforcement organizations to obtain evidence concerning places to be searched, objects to be seized, or persons to be arrested.

e. Information. Information obtained by the USACIDC in the course of an investigation under DoD Directive 5525.7, including information obtained about non-DoD personnel, may be provided to civilian law enforcement officials and appropriate prosecutorial authorities. Personnel assigned to or under the control of the USACIDC may testify concerning such information in DoD and non-DoD judicial and administrative proceedings. Paragraph 7-3, AR 27-40, details the requirements for DA military m embers or certain employees to follow before testifying in a certain court or hearing. Field elements should contact the respective USACIDC major subordinate command judge advocate for further guidance.

13-35
Approvals

Controlled purchases of illegal drugs outside of military installation in CONUS from persons not subject to the UCMJ require the prior approval of the respective USACIDC major subordinate commander following a legal review of the re quest by the USACIDC major subordinate command judge advocate. In the absence of the USACIDC major subordinate commander, the USACIDC major subordinate deputy commander is authorized to approve the request. This authority may not be further delegated .

13-36
Coordination

Off post CONUS drug investigations by USACIDC involving persons not subject to the UCMJ and controlled purchases from these persons outside of military installations will be coordinated with:

a. The appropriate federal, state, or local law enforcement agency. Whenever possible, these investigations will be conducted jointly with these civilian agencies.

b. The appropriate U.S. attorney or state or local prosecutor.

c. The supporting staff judge advocate.

13-37
Request for approval

Request for approvals of controlled purchases of illegal drugs, which are to occur off post in CONUS or which involve persons not subject to the UCMJ in CONUS, will be forwarded by the most expeditious method to the respective USACIDC major subordinate command. Requests will contain, as a minimum, the following information.

a. The USACIDC ROI or sequence number.

b. Information concerning the seller (target) and the military connection of the controlled purchase. This section should identify the seller(s) to the maximum extent possible. It is not necessary to possess a complete identification and name of the subject so long as the available information is sufficient to distinguish the subject from the general population. The information must identify

the facts and circumstances constituting reasonable grounds to believe that the seller:

(1) has committed a drug offense in conjunction with a member of the Armed Forces, or,

(2) is the immediate source of the introduction of illegal drugs onto the military installation. A location such as a bar or street corner identified as a known distribution point to soldiers may not be a target.

c. Justification for the use of military law enforcement personnel, including an explanation of why civilian law enforcement agencies are unable or unwilling to conduct the investigation without CID involvement.

d. The investigative plan. This section should describe, in detail, the plan coordinated with the civilian law enforcement agency. If multiple purchases are anticipated, this should be stated together with the reasons for such purchases (e.g., the civilian prosecutor will not accept a case for prosecution with less than two controlled purchases). Information should also be included concerning the civilian agency's willingness to effect apprehensions, serve warrants, and conduct searches.

e. Desired length of approval. The maximum length of time in which to complete approved controlled purchases is sixty days. Subsequent extensions of this time period may be approved by the USACIDC major subordinate commander. To ensure continuity of a particular operation, requests for such extensions should be received at the USACIDC major subordinate command no later than five working days before the expiration of current approval.

f. Statement of coordination and concurrence. This section must reflect coordination with the appropriate civilian police agency and the supporting staff judge advocate, and the U.S. attorney or state or local prosecutor as appropriate. Concurrence may be obtained telephonically. Coordination must be accomplished and concurrence obtained for each separate investigation and may not be done by a memorandum of understanding covering a general category of investigations.

g. A point of contact for notification of approval or disapproval of the request.

13-38
After-action reports

For each request for controlled purchases approved under this section, an after-action report will be submitted by the most expeditious method to the USACIDC major subordinate command within five working days of termination of the

investigation, inclusive of any extensions granted, and will be in the format listed below:

a. Sequence/ROI number: Include the USACIDC major subordinate command document control number in parenthesis, if applicable.

b. Name and disposition of offender: Include as much possible information (i.e., arresting agency and date, incarceration, trial, etc.)

c. Type and quantity of drugs seized.

d. Total CID funds expended. This should also include surveillance expenses, as well as any other expenditures incurred in support of the investigation being addressed.

13-39
General

Section 881 (A)(4), Title 21, United States Code, provides for the seizure and forfeiture of any vehicle or other mode of transportation which is used or intended to be used to transport or facilitate the transportation, sale, receipt, possession or concealment of all controlled substances which have been manufactured, distributed, dispensed or acquired in violation of Title 21, USC.

13-40
Authority of the DEA

The DEA has been authorized and designated to make seizures of property by the provisions of 21 CFR 1316.72 and is authorized to make disposition of forfeited property by 21 USC 881(E)(4).

13-41
Policy

a. The fact that military investigative authorities initially identify a vehicle or lawfully seize a vehicle used for the purposes outlined in paragraph 13-39 does not affect the DEA's authority to institute forfeiture proceedings. There is no prohibition against USACIDC establishing liaison with the DEA and providing information to them so action under 21 USC 881 may be initiated if the DEA deems it appropriate.

b. The following guidelines are provided regarding vehicles subject to forfeiture under 21 USC 881(A)(4):

(1) Coordinate with the local DEA office to determine the amount of controlled substance and circumstances which would cause the DEA to institute forfeiture proceedings.

(2) Promptly notify the local DEA office when a motor vehicle (subject to forfeiture under 21 USC 881) is seized by military authorities for reasons other than seizure under 21 USC 881. If the DEA is going to initiate forfeiture act ion, the vehicle, when no longer needed for military investigative purposes, will be immediately turned over to the DEA. A vehicle seized for military investigative purposes, for which the DEA has not instituted forfeiture proceedings, will be returned to the owner when no longer required by military authorities.

(3) Military investigative authorities will not physically seize motor vehicles (e.g., in the absence of a military interest to do so) for purposes of forfeiture action under 21 USC 881. Seizures under such circumstances would be contrary to the terms of the Posse Comitatus Act (18 USC 1385).

Figure 13-1. Controlled Substance Measurements and Conversions

Controlled Substance Measurements and Conversions

a. The metric system will be used for recording and reporting all weight, volume, and linear measurements of seizures of controlled substances.

b. Common use measurements and conversions:

kilogram = 1,000 grams or 2.2 pounds
gram = 0.035 ounce
milligram = .001 gram or 0.000035 ounce
liter = 1.16 quarts
centiliter = .01 liter or .338 fluid ounce
milliliter = .0001 liter or 0.034 fluid ounce

meter = 39.37 inches
centimeter = .01 meter or 0.39 inch
millimeter = .001 meter or 0.039 inch

2.2 pounds = 1,000 grams
1 pound = 453.59 grams
1 ounce = 28.35 grams

1 gallon = 3.78 liters
1 quart = 0.95 liter
1 pint = 473.17 milliliters
1 fluid ounce = 29.60 milliliters

1 yard = 0.91 meter
1 foot = 0.31 meter
1 inch = 2.54 centimeters

Figure 13-1. Controlled Substance Measurements and Conversions

DST Standing Operating Procedure (SOP)

1. General

a. The purpose of the SOP is to enumerate those procedures which are unique to the organization and which are habitually used for accomplishing routine actions.

b. The DST SOP will provide operational guidance in the conduct of drug suppression activities of special agent super- visors, special agents, MP and non-MP personnel assigned, attached or detailed for duty with the DST.

2. Scope

a. Each DST should develop a SOP based on the desires of the battalion/field office commander and habitual procedures that have been developed through experience.

b. The DST SOP will only include procedures unique to the drug suppression operation and will normally be an addendum to the CID office SOP.

c. The SOP will be changed, as necessary, to meet various conditions or existing practices. The SOP will be sufficiently complete to advise attached DST members of the procedures followed by that CID unit. The amount of detail depends of t he size of the team and its state of training.

d. The SOP will not be used to consolidate directions and procedures prescribed in other publications and documents available to the drug suppression team.

3. Responsibilities. Determination of necessity, preparation, publication and distribution of the DST SOP is the responsibility of the battalion/field office commander.

CHAPTER 14

14-1
Purpose

This chapter clarifies and gives guidance on the recruitment and management of registered sources, sets forth a suggested source management process with a ledger and automated Master Source File (MSF) contained within the Criminal Intelligence (CI) module of the Automated Criminal Information Reporting System (ACIRS); outlines coordination on fear of life transfers; gives guidance on recruitment and use of juveniles as sources; and clarifies USACIDC requirements when an Article 32, UCMJ board officer, defense counsel or judge seeks disclosure of a registered source's identity.

14-2
Explanation of Terms

a. Source. A person, from whom information is obtained and/or who assists CID agents during an investigation. Sources may be open or registered. Their identities require some degree of protection (see paragraph 14-9). Dependent upon specific circumstances, sources may be considered as "agents of the U.S. Government."

b. Open Source. An individual who may be fully identified in discussions or correspondence without protecting his identity, such as a first sergeant, a unit commander, a finance clerk, or a willing witness.

c. Registered Source. An individual who is recruited and targeted by a CID agent to covertly gather intelligence for USACIDC. A registered source may also be an individual who is willing to provide intelligence on occasion, but has requested anonymity. A person who knowingly and willingly provides information to a CID agent but is unwilling to be registered, will nonetheless be handled and processed as a registered source. There is no requirement to notify an individual that he will be processed as a registered source. Registered sources are always considered agents of the government and their identity will be protected.

d. Unwitting Source. A person who provides information without being aware that the person he is dealing with is a CID agent. There is no requirement to notify an unwitting source that he will be processed as a registered source.

e. Source File. A controlled access file pertaining to a single registered source, maintained at the local USACIDC unit. The file need only contain the source's CID Form 20 (Source Data Card), a Declaration of Understanding (if initiated), and any other documents deemed appropriate or administratively needed (i.e., sworn statements, receipts, photographs, etc.). Source activity documented on an Agent's Activity Summary (AAS) maintained in another investigative file need

not be reproduced or appended to the source file, but there may be a cross reference notation.

f. Master Source File. An automated file within the criminal intelligence module of ACIRS or a physical file, accessible to CID agents/investigators only, which is maintained at each USACIDC unit and contains information about sources used by that unit.

g. Primary Handler. Any USACIDC agent, investigator or investigative operations assistant who directly controls a particular registered source's activities.

h. Alternate Handler. Any USACIDC agent, investigator or investigative operations assistant who assumes the responsibility for a particular registered source during the temporary absence of the primary handler.

i. Source Control Officer (SCO) and Alternate SCO. The USACIDC agents, supervisors or civilian employees who coordinate all source matters, maintain local source files, and provide guidance to unit personnel on source management.

j. Source Registry Officer (SRO) and Alternate SRO. The USACIDC agents, supervisors, and civilian employees located at HQUSACIDC who supervise the USACIDC source program and who maintain the Central Source Register (CSR).

k. Triggering Event. A significant event during the relationship between a registered source and the recruiting USACIDC unit that requires the unit's SCO to forward the source's Source Data Card to the HQUSACIDC SRO. Such an event may be the termination of a registered source, a transfer of a source from one USACIDC unit to another, the need to initiate a fear of life (FOL) transfer, or some other significant event.

14-3
Responsibilities

a. The Deputy Chief of Staff for Operations (DCSOPS), HQUSACIDC, will:

(1) Provide the command and staff supervision of the USACIDC Source Program.

(2) Assist field elements in the implementation of the USACIDC Source Program.

(3) Designate a Primary and Alternate SRO.

b. The Policy Branch, HQUSACIDC, will establish policy effecting the implementation and operations of the USACIDC Source Program.

c. Director, Crime Records Center, will provide information to USACIDC elements IAW paragraph 14-8b(6) below.

d. Inspector General, HQUSACIDC, will evaluate the quality of source management based on its incorporation into a USACIDC unit's Criminal Intelligence Program and its overall effectiveness in detecting, preventing and solving crime.

e. The Primary and Alternate SRO will:

(1) Manage and coordinate the USACIDC Source Program and complete staff actions related to source matters.

(2) Maintain the CSR IAW this chapter.

(3) Coordinate all requests for transfers initiated under the source transfer program IAW paragraph 14-10 below.

(4) Respond to all inquiries from authorized personnel and agencies concerning anyone who has worked, or allegedly worked, as a source for the USACIDC.

(5) Identify and locate reliable registered sources with specialized capabilities needed for a specific mission. Then, if necessary, coordinate with the Total Army Personnel Command (TAPC) to arrange the transfer of the source to the required location.

f. Commanders of USACIDC major subordinate commands (MSC) will:

(1) Establish an effective, comprehensive and balanced source program involving active participation of subordinate commanders and supervisors.

(2) Coordinate with HQUSACIDC, as necessary, to make changes to existing source handling procedures.

(3) Designate a staff coordinator to monitor the source program and ensure that a primary and alternate SCO is appointed at each battalion/field office and designated resident agencies.

(4) Ensure files are established and maintained IAW AR 25-400-2, the Modern Army Record-Keeping System (MARKS).

(5) Ensure adequate .0015 funds are requested to support the source program.

g. CID supervisory personnel in USACIDC field units:

(1) Ensure a quality source program is developed and implemented within their area of responsibility.

(2) Designate primary and alternate SCOs at subordinate units and oversee their activities to ensure compliance with this chapter.

(3) Ensure each active registered source has a primary and alternate handler designated to control their activities.

(4) Receive a briefing on the overall effectiveness of the source program from the SCO after each quarterly SCO file review and inventory. No entries in the files are required to document this briefing.

h. The Source Control Officer (SCO) will:

(1) Establish the USACIDC source management program IAW this chapter.

(2) Advise primary and alternate source handlers on current USACIDC source management policies and procedures.

(3) When required by a triggering event, submit a current source data card IAW Figure 14-1 within 30 days if OCONUS or 15 days if in CONUS to HQUSACIDC, ATTN: CIOP-IN-SRO, for each registered source impacted by the event. The source data card will be sent via certified mail, return receipt requested, marked "SRO EYES ONLY.” When the triggering event is time sensitive, the telefaxing of the source data card to HQUSACIDC is authorized.

(4) When credible threat information has been confirmed, notify the SRO of a FOL transfer situation IAW paragraph 14-10 below.

(5) Submit a copy of the source data card to the SRO on all registered sources at the time of inactivation. These forms will be submitted within the same time frames indicated in paragraph 14-3h(3) above.

(6) Maintain source files in a locked file cabinet, with access controlled as required in paragraph 14-15 below.

(7) Maintain other correspondence directly relating to registered sources in a secure container.

(8) Maintain the MSF as required by this chapter.

(9) Maintain appropriate control methods, such as a source log, and assign source code numbers to newly recruited sources IAW this chapter.

(10) Conduct a quarterly inventory to review active source files and brief supervisory personnel after each review summarizing the status of the source program.

(11) Ensure that local USACIDC supervisory personnel are apprised of significant deficiencies and changes in the source program.

(12) Ensure that registered sources are reassigned to other agents prior to the PCS or ETS of the primary or alternate handlers.

(13) When applicable, coordinate with the gaining USACIDC unit regarding the PCS of a registered source to ensure continued use. This may include sending the gaining CID element a copy of the source data card, a copy of the PCS orders, and a brief introduction.

i. Primary or alternate source handlers will:

(1) Conduct assessments of criminal incidents reported, criminal intelligence gathered, crime prevention surveys performed, historical data on file concerning criminal incidents, and the potential for criminal activity, in order to initiate source recruitment efforts in certain facilities, covering the entire spectrum of criminality.

(2) Initiate and update individual source files IAW this chapter.

(3) When applicable, assist registered sources in the resolution of personal problems, but only when these matters develop as a result of the source's association with the USACIDC.

(4) Assist in the transition of registered sources to new handlers prior to the source handler's departure, when applicable.

14-4
General

The USACIDC Source Program is designed to standardize the coordination of source related activities of all USACIDC elements.

a. The recruitment, use, control and termination of sources are governed by policy as stated in this chapter. The USACIDC source management program includes open and registered sources.

b. The source program of each USACIDC unit will be evaluated in terms of its ability to develop and use sources who contribute criminal intelligence from which criminal investigations are initiated; subjects identified; and criminal activity detected, reduced, solved or prevented. The administrative requirements of this chapter are designed to promote the efficient recruitment and effective management of sources and to facilitate the investigative process. Compliance with the administrative portions of this chapter will not, in itself, be considered as evidence of a successful source program.

c. The intent of this program is to develop, target as necessary, and utilize quality sources in all types of criminal activities.

d. The sensitive nature of the source program and the potential danger to sources, if compromised, dictate that all aspects of source management be conducted with extreme care and discretion.

14-5
Source Management

a. Initial contact and recruitment of sources is accomplished primarily by persons performing investigative duties for the USACIDC. Each registered source is assigned to a handler who is responsible for maintaining contact with the source, tasking and targeting the source, and exercising appropriate control over the source's official activities. The handler will systematically debrief the source, relay information provided to those best able to use it and ensure that a file is maintained which reflects the source's current status and activities. The relationship between the source and the handler creates legal, moral and administrative responsibilities for both the USACIDC and the handler. This relationship requires that all reasonable measures be taken to protect the registered source's identity and that only individuals capable of providing information within the spirit of this chapter are classified as registered sources.

b. Source activities within USACIDC units are managed and coordinated by the SCO, who may also serve as the unit’s criminal intelligence coordinator.

(1) SCOs, in conjunction with field operations officers, will emphasize recruitment of sources. As appropriate, they will review selected open cases, inquiries and surveys to monitor and encourage the use of sources.

(2) The SCO is responsible for conducting quarterly inventories and review of all active registered source files. During reviews, the SCO will ensure that files contain appropriate documents, that records of performance are recorded or maintained, and that necessary coordination is being conducted with the SRO when needed.

(3) SCOs and CID agents will direct source efforts toward the development of criminal intelligence.

(4) SCOs should ensure that handlers are using only those sources who contribute or have the potential to contribute useful information. The termination of a source will not be based merely upon inactivity. To continue or terminate a source is a subjective determination made collectively by the USACIDC supervisory personnel and the source handler. Future potential use must be given adequate consideration during the determination. A registered source may be dormant and still be considered of value because of his position.

(5) SCOs will coordinate, when necessary, directly with the SRO.

c. Coordination of source matters at HQUSACIDC level is the responsibility of the SRO.

(1) The primary duties of the SRO are to manage the USACIDC Source Program, conduct liaison with USACIDC field units and their SCOs, answer requests for information on availability of sources assigned to other CID units, and to receive and ensure the posting of updates provided by SCOs for the CSR.

(2) The SRO is the POC between the USACIDC and Department of the Army (DA).

(3) The SRO is responsible for the maintenance and confidentiality of the CSR.

14-6
Planning and Goals for Source Operations

a. Planning for operations must include a realistic assessment of crime conditions prevalent in the CID unit's area of operations. Such concerns as soldiers, family members, civilian employees, crime trends and rates, criminal profiles, and ethnic and racial divergence must be considered when initiating and maintaining an active source recruitment program.

b. A balanced network of sources, military and civilian, should be recruited from all segments of the available population to provide information on all criminal activity taking place in those areas where there is a definite military connection. Measures should be implemented to recruit and retain a balanced network of sources encompassing all crime areas, consistent with the local investigative priorities. The provisions of paragraph 14-8c(8) below will apply for sources under the age of majority.

c. Arbitrary quotas or goals of sources will not be imposed, implied, or directed.

14-7
Information Sources

a. The term “information source” has a broad meaning encompassing many possible origins of information. Some sources may be classified as witnesses if their information is provided openly and aids the CID agent in an investigation. Some individuals providing information may need to have their identity protected. These individuals should be classified as registered sources when:

(1) An individual requests anonymity.

(2) An individual’s actions in regard to investigative efforts are controlled or targeted by a USACIDC unit, even on a one-time basis.

b. For personal convenience, CID agents may maintain a database, card file, directory book or log containing the names, units and locations of all sources to whom they have access. In keeping with the Army Privacy Program, such records may not be physically released to an agent's successor or to any other person. However, the information contained within these personal records may be passed on for official use as appropriate. Agents are cautioned not to maintain such records on their person while engaged in criminal investigative activities.

c. Files, notebooks, and so forth, maintained by agents for personal convenience, and which contain sensitive information regarding sources, should be secured and protected from compromise at all times.

d. To facilitate management of sources used by a unit and to allow for the most effective overall use of such sources by the agents within the unit, the SCO will maintain a filing system, referred to as a "master source file." This file may be categorized by names, post locations, units, or crime areas. The MSF will consist of a computerized listing or index type cards system covering open and registered sources. Under any given category, such as a unit designation, all sources of information within that unit will be found. Open sources, such as the unit commander, first sergeant, or clerks, will be listed by location, name, and handler, and will be available to agents for open contact (Figure 14-2). Registered source cards or computerized system will list, as a minimum, the source's unit or location of employment, source number, and handler's name (Figure 14-2). Actual identity of registered sources will not appear in the MSF. Should an agent desire the use of a registered source listed in the MSF, the agent should contact the SCO for the identity of the handler. The agent then would contact the handler, at which time the handler and agent will decide on the proper employment and use of the source. The MSF will not contain any other information, and access to the MSF will be controlled by the SCO.

14-8
Recruitment and Utilization of Registered Sources

a. General.

(1) Guidance pertaining to the management of registered sources is included in detail in Appendix M. These procedures are meant as a guide and are subject to modification in order to tailor them to individual USACIDC unit circumstances. All possible situations and factors involved in source management cannot be included in a regulation or field manual. As in any interpersonal relationship, CID agents must rely largely on experience and professional judgment when dealing with sources.

(2) Individuals furnishing information to the USACIDC should be classified as sources of information and formally registered if any of the following criteria apply:

(a) An individual is recruited for the purpose of covertly gathering information, identifying suspects, purchasing illegal contraband, or performing similar covert activities while associating with and maintaining contact with the criminal elements.

(b) Control procedures or instructions are provided to the individual by USACIDC agents to specifically and actively gather intelligence about a particular criminal situation or suspect.

(c) A source increases activities to a degree where:

1. It becomes necessary to pay or reimburse a source with .0015 funds.

2. Measures and controls are instituted to ensure the physical safety of the source.

3. An individual is routinely providing the USACIDC with valid and useful criminal intelligence information obtained through contact with criminal elements and his identity needs to be protected.

4. It is the judgment of the source handler that any of the above is likely to occur or the registration of an individual as a source will be beneficial to the USACIDC mission.

(d) An open source requests anonymity in exchange for information provided.

b. Recruitment.

(1) Recruitment efforts will be considered adequate if:

(a) The registered source system contributes to the success and effectiveness of the investigative mission. The quality and productivity of open and registered sources are critical to the effectiveness of the source program.

(b) Active registered sources, although not used frequently, are in positions for future usefulness based on the documented targeting priorities of the unit.

(c) The base of active registered sources reflects a potential for usefulness which spans different crime areas, locations or trends.

(2) Upon recruitment of a registered source, either directly or through an upgrading of the status of an open source, the individual may be advised of his designation as a registered source. However, there is no requirement, legal or otherwise, to notify a source that he will be registered or that he is a registered source.

c. If a registered source, who possesses specific skills, is needed to assist in the conduct of a particular operation and efforts at the local level to recruit such a registered source have proven unsuccessful, assistance can be requested from the SRO. This request should contain the following information:

(1) Type of operation contemplated.

(2) Expected duration of the operation.

(3) Registered source requirements, such as specific MOS, language ability, special training or ability.

(4) Name of the primary handler and the manner in which the registered source should make initial contact with the CID agent assigned as his handler.

(5) Desired date of registered source availability.

(6) Summary of investigative efforts to date.

(7) Other special considerations, if appropriate.

d. Some personnel within the U.S. Army military intelligence (MI) community possess special intelligence (SI) clearances. In using these personnel as sources, continuing coordination should be conducted with the local MI unit to preclude compromise of sensitive information. At the time when these personnel are recruited, notification will be forwarded to the SRO via a source data card, including coordination made and that the source possesses a SI clearance. This requirement is not intended to negate or restrict the use of information furnished

by an individual who possesses a SI clearance, when that information is unsolicited and relates to a particular criminal offense or investigation.

e. The Army Substance Abuse Program (ASAP) prohibitions and restrictions are defined in AR 600-85. USACIDC CID agents and other investigative personnel, to include sources, will not solicit information from ASAP participants. Information which is volunteered is acceptable, as long as it is not obtained within an ASAP facility or in such a manner as to jeopardize the safety of the source or in a way which compromises the credibility of the ASAP. No covert agents or sources will enroll or infiltrate ASAP facilities for the purpose of law enforcement activities. The USACIDC agent must know if their source(s) are ASAP participants.

f. Crime Records Center (CRC) checks must be performed on all registered sources. Results of this check will be recorded in the remarks section of the source data card. Sources may be used prior to the receipt of a response from the CRC, if it is determined necessary by the handler and the SCO. Record checks on registered sources require the following:

(1) Provide the CRC with the monthly criminal intelligence raw data file (RDF) sequence number.

(2) List the reason for the check as "regarding criminal investigation activities" only.

(3) Record the date and agent's name on an AAS in the RDF with the comment, "Records check on registered source (CID -)." Do not use the name of the source on the AAS , only the source number. Do not index the information other than in the source's file folder.

(4) Record the results of the records check in the appropriate block on the source data card in the source's folder, block 51 (Remarks).

(5) Hard copies of negative results on name checks are not required.

g. The polygraph can be a valuable aid in determining the veracity and reliability of a source. Although sources cannot be required to submit to a polygraph examination, its use should be considered when circumstances indicate the results may be valuable in evaluating a source and the information he/she provides. The prerequisites of AR 195-6, Department of Army Polygraph Activities, must be met in each case. Although not an all inclusive list, the following situations may be suitable for offering polygraph examinations:

(1) A newly developed source whose credibility cannot be otherwise evaluated provides information concerning significant criminal activity.

(2) An established source provides information which, if true, would lead to a covert or other operation involving the commitment of significant CID resources.

(3) An unsubstantiated FOL may require a polygraph examination to determine the actual need of a FOL transfer.

(4) A source whose reliability has been questionable in the past provides information about significant criminal activity.

h. Registered Source Use

(1) Registered sources must be controlled to ensure all aspects of those actions in which they are involved reflect proper investigative procedures. The fact that sources are not familiar with acceptable investigative techniques requires that handlers convey to sources a clear understanding of what is expected of them and what they can expect from USACIDC. Guidelines regarding such measures are outlined in Figure 14-3. An annotation will be made in the remarks section of the source data card reflecting that applicable topics contained in the guide were discussed with the source, or a copy of the Declaration of Understanding (Figure 14-4) may be included in the individual source file. For unwitting sources, the completion of an understanding discussion is not required, but an annotation to that effect will be entered in the remarks section of the source data card.

(2) There are a number of factors CID agents should consider prior to soliciting or using the services of a registered source: the motives of the source; the potential benefit to be derived from the source's efforts; the knowledge and contacts of the source in the crime area of intended use; any past examples of reliability and/or unreliability (unit commander, local police, other CID elements); any problems (personal, administrative, or otherwise) which could affect the source's performance; and any anticipated risk or compromise of the source's identity or safety.

(3) All active registered sources must be registered and documented as provided in this chapter.

(4) To ensure maximum and future productivity, all active registered sources will be contacted as often as necessary. The determination of how often a source should be contacted will be determined by the handler with advice and guidance from the SCO, and CID supervisory personnel. Overall productivity of this program is directly influenced by the interpersonal relationship between the handler and the source.

(5) During the course of source contacts, the handler should evaluate the source's motivation, attitude, morale, sincerity, productivity and potential for future productivity. If no useful information or assistance has been provided by

the source during the preceding 90-day period (or even since the last contact), and the handler and SCO judge that there is little potential for such information or assistance being furnished in the future, the use of the registered source should be terminated and the source file placed in an inactive status. The inactivation of a registered source is a triggering event requiring the forwarding of source data card to the SRO. Should such a source resume productivity at some later date, the individual can be reactivated using the same source number and file. In these instances, an updated source data card will be forwarded to the SRO to reactivate the source in the CSR.

(6) Some sources are motivated by matters which result in a judicial or administrative elimination proceeding. Caution should be exercised in using military personnel as sources if they are involved in judicial or administrative proceedings. Special care should be taken and appropriate coordination conducted in these situations, to avoid unnecessary delays or interruptions in such proceedings. If a delay should prove necessary because of the information being provided, then the handler must coordinate closely with the SJA and/or the appropriate approving authority.

(7) No promises will be made to sources which require the action of some other authority. For example, it is appropriate for a handler to advise a source that the trial counsel in his case will be informed of the source's cooperation; however, promises concerning contemplated judicial action, dismissal of charges or cancellations of judicial proceedings cannot be made by sole authority of USACIDC personnel. It is inappropriate to promise a source that he will be reassigned to a more desirous location because of his work for the USACIDC.

(8) Civilian personnel under the age of majority may be used as USACIDC open or registered sources. Before a minor is used, approval must be obtained from the SCO and USACIDC supervisor. A written certificate (figure 14-5) giving permission to use the minor as a source will be obtained from the minor's parent or legal guardian. The recruitment of a minor as a registered source is a triggering event. The original of the certificate will be filed with the source data card. A duplicate certificate, along with the source data card, will be forwarded to CDR, USACIDC, ATTN: CIOP-IN-SRO, for inclusion in the CSR. Additionally, the source data card will be annotated indicating the approval of the unit SCO and supervisor. In most jurisdictions, the age of majority is 18; however, coordination will be made with the supporting SJA to determine local law.

(9) Military police investigators (MPIs) generally will not be registered or used as registered sources. Military police (MP) and correctional specialists may be registered in the case of sensitive investigations. The registering of MPs as registered sources will only be accomplished when it is the only feasible means of obtaining critical information or infiltration of a group involved in a sensitive investigation.

(10) Documentation on the AAS, contained in the case files (ROI or CIR), will reflect, as appropriate, source activities and the details of related contacts made with sources.

(11) References to sources and their activities in AASs, evidence custody documents, or .0015 fund vouchers (i.e., internal documents), will always be recorded by the source number. References to a source in an AIR or ROI (i.e., external documents) will simply be "source" or "CID source." No registered source numbers will be used on external documents.

14-9
Protection of Source Identity

a. Anonymity must be furnished to all registered sources who, regardless of motive, have provided USACIDC with information concerning the criminal activities of others. Anonymity can normally be provided by restricting the release of the identity of a registered source, exercising appropriate security measures regarding communications between the registered source and the handler, and by using caution in documenting their activities on external documents. Additional protective measures may become necessary, predicated upon the situation at hand. These measures may include providing physical protection and/or transferring an individual to another location. However, no guarantees will be made concerning possible transfers or the locality of any forthcoming assignment. USACIDC policy is to protect, to the maximum extent provided by law, the identity of any legitimate source.

b. The following guidance concerns the protection of a source's identity as allowed under the Military Rules of Evidence (MRE)

(1) The confidentiality of a source's identity is a limited privilege recognized by military law. MRE 507, MCM 2001, provides that a source's identity is normally privileged against disclosure. Communications of these individuals are also privileged to the extent necessary to prevent disclosure of their identity. This privilege, however, is not absolute and is subject to various exceptions. Legal considerations in this area are both complex and subject to change. Accordingly, continual liaison is particularly important when, due to operational considerations, a local USACIDC unit determines that non-disclosure may result in a dismissal of charges or an accused's acquittal at trial. Local USACIDC supervisory personnel will present any such determination, along with supporting facts and rationale, to the servicing trial counsel, Chief of Military Justice or, if necessary, the appropriate SJA at the earliest possible opportunity. Every effort will be made to ensure a USACIDC/SJA agreement has been reached on the disclosure issue prior to the commencement of court-martial proceedings (i.e., before the preferral of charges). Disagreements which cannot be resolved at the local levels will be forwarded for resolution to the appropriate higher headquarters. Early

coordination on this issue will prevent needless delays or embarrassment to the Government during court-martial proceedings.

(2) At trial, all disclosure orders made by a military judge will be complied with fully. However, in an appropriate case, such as where disclosure may jeopardize an important ongoing investigation, USACIDC may request, through the trial counsel, a recess to petition the convening authority to terminate the current judicial proceedings. If the convening authority will not terminate the proceedings and the military judge will not reconsider his order to disclose, the disclosure order will be complied with and the SRO will be notified immediately. Coordination should be made with the trial counsel to prevent excessive disclosure of information not material or necessary for the adequate defense of an accused. To this end, USACIDC will, through the trial counsel, request the military judge to conduct an in camera examination of all source information prior to ruling on a request for disclosure.

(3) Requests from other than a military judge to disclose the identity of a source in the course of military judicial proceedings (Article 32b, 39a, etc) will be honored only after consultation and agreement between the USACIDC, the source handler and the supporting SJA. If serious disagreements arise between the USACIDC and the local SJA, the USACIDC will withhold release of the information and immediately forward the request to the USACIDC MSC SJA and, if necessary, to the OSJA, HQUSACIDC for further resolution.

(4) Once a source's identity has been disclosed, release of all additional non-classified information concerning the source falls within the government privilege set forth in MRE 506. Only the Secretary of the Army has the authority to exercise this privilege and deny disclosure of any such information maintained by this command. It is always appropriate, however, to consider requesting the trial counsel or military judge to review, in camera, all source information prior to disclosure to prevent excessive release of information not essential to the defense of the accused.

(5) Whenever there is a request for the identity or release of communications which could lead to the identity of a source, a careful analysis must be made of the relevant facts. This analysis should be made in conjunction with the local legal advisor or servicing SJA.

c. The following guidance is applicable regardless of whether the request for disclosure is made under the MRE or through civilian authority.

(1) Normally, when a source is used by USACIDC agents to purchase drugs or other contraband directly from a suspect, and prosecution is intended, anonymity of the source's identity cannot be maintained and the source will be required to testify at some point. In such instances, sources should be made aware of this prior to providing information. Conversely, where a source's only contribution is to

introduce a covert agent or another source to a suspect, the probability of the USACIDC unit being compelled to release the source's identity or the source being compelled to testify is diminished.

(2) Requests for release of a source's identity from another investigative agency, or made pursuant to a civilian administrative or judicial proceeding, should be referred immediately to the SRO or the MSC SJA for resolution on a case-by-case basis. The guidance applicable to disclosure under MRE will be applied, as appropriate, when disclosure is at issue in civilian courts. Local USACIDC supervisors will contact their USACIDC MSC SJA for advice and as a POC for the civilian prosecutor. Where an SAUSA has been designated to the installation SJA, this officer would be contacted as an additional source of information and point of contact with the civilian prosecutor. Any disclosure of a source's identity to authorities external to the USACIDC must be documented in the source file and by source number only in the AAS of the case file.

d. Sources will be provided security when necessary for their physical protection, IAW paragraph 14-9, when:

(1) The local USACIDC unit determines a threat of physical harm to a source warrants special protective measures. The validity and severity of the threat will be determined through initiation of a CID preliminary inquiry or ROI. The results of this inquiry will be annotated in the source file.

(2) The threat evaluation verifies that a threat was actually made or that, in the absence of an overt threat, there exists significant evidence indicating the possibility of physical harm to a source.

(3) The threat appears to be legitimate, and the source must remain in secure surroundings. The source's commander will be notified immediately. This notification is intended to protect the source from possible punitive action that could result from any absence from assigned duties.

e. Non-military sources of information (DA civilians, family members, host country/third country nationals, local civilians, etc.) will be protected and alleged threats evaluated in essentially the same manner as those against military sources. However, in such cases, liaison should be made immediately with local, foreign or Federal civilian law enforcement authorities as appropriate. Where a threat to a civilian source cannot be resolved through appropriate liaison and contact with civilian authorities, coordination will be made with the SRO.

14-10
Transfer of Sources

a. Military sources and witnesses may be transferred as a result of potential or real threats to their safety. The USACIDC unit confirming a real or potential threat to life situation on behalf of a source or witness incurs the responsibility of ensuring the safety of this individual until such time as the situation is resolved and the soldier departs the installation. The USACIDC unit will take all actions deemed reasonably necessary to ensure the safety of a source and/or witness in a FOL situation. Contingency limitation .0015 funds should only be used to secure an individual's (military personnel and their family members) safety from the time the threat is received until the necessity for a FOL transfer has been verified. After the need for a FOL transfer has been verified, the military PCS system should be used to cover such costs as Temporary Living Allowance, Basic Allowance for Subsistence, etc., unless the provisions of AR 195-4 can be justified. FOL cases involving civilian sources and witnesses are more complicated and coordination should be made with the SRO for guidance.

(1) Prior to transfer, sources will normally be debriefed IAW paragraph 14-11b below.

(a) If a registered source being transferred indicates an unwillingness to serve as a source at the location of next assignment, the nearest USACIDC unit will be notified of the deactivated source's impending arrival for criminal intelligence purposes. This is necessary in the event that threat situations or problems arise with the individual at some later date. The details of notification should be annotated in the source file of the losing USACIDC unit and the criminal intelligence files of the USACIDC unit nearest the deactivated source's new assignment. Copies of documents in the source file may be forwarded to the gaining unit at their request.

(b) If the source indicates a willingness to work for the USACIDC at the new location, the primary source handler or the SCO will forward to the gaining unit a copy of the source's data card and copies of any other documents contained in the source's file deemed appropriate and pertinent for the continued use of the source. These documents will be sent by certified mail, return receipt requested, ATTN: SCO, with the envelope marked "Eyes Only-SCO." Original source related documents may be forwarded to the gaining unit upon request with copies retained in accordance with AR 25-400-2 by the losing unit. Prior to being integrated into the source program of the gaining unit, the source will be evaluated and, if acceptable, issued a new source code number. A copy of the new source data card will be forwarded to the HQUSACIDC SRO referencing the old source number. Documentation received from the losing unit will be included in the new source file.

b. Registered sources may be transferred into an area within the boundaries of investigative responsibility of a particular USACIDC unit, but assigned for duty to a facility supported by another Defense Criminal Investigative Organization (DCIO). In the above circumstances, the losing USACIDC unit will notify the SRO of the history of the source's service and willingness to continue employment as a source. The SRO will then determine the potential value of the source to the other DCIO and notify that agency, if appropriate.

c. Records of registered sources who are transferred will be deactivated in the files of the losing USACIDC unit. These files will be disposed of IAW AR 25-400-2.

d. Threat transfers (CONUS),

(1) When a USACIDC unit confirms that there is a credible threat to the safety of a source (see paragraph 14-9 above) and a transfer from the installation is deemed necessary to assure the protection of the source, the local SCO will accomplish the following:

(a) Notify the source's commander of the impending move and determine if the commander concurs with the move. Should a conflict arise between the unit commander and the USACIDC unit, the battalion or field office commander should resolve the conflict with the soldier's higher chain of command. Declinations will be documented in a MFR showing relevant facts and circumstances.

(b) Notify the SRO of the FOL action and provide the relevant facts and circumstances pertaining to the action (Figure 14-4). The SRO will coordinate with the TAPC.

(2) The SRO will obtain the source's new assignment and notify the initiating SCO, to include local military personnel office (MILPO) designated POC.

(3) In special circumstances, subject to review by the SRO and a verified need by the USACIDC for the continuing services of a registered source, a specific unit of assignment, at the request of USACIDC, may be obtained. Consideration pertaining to a USACIDC influenced assignment on behalf of the registered source will be based on review of all circumstances relevant to the request, a specific need by the USACIDC for the continued services of the registered source, willingness of the source to assist the USACIDC at his new duty assignment and the past performance record of the registered source. The USACIDC influenced FOL transfer actions where a specific unit of assignment is requested, will not be construed to be a routine action and will be based on a review of all circumstances on a case-by-case basis and the overall needs of the USACIDC.

(4) When a USACIDC requested specific unit of assignment is obtained under a FOL situation, coordination with the gaining USACIDC unit will be made by the losing USACIDC unit regarding the arrival of the registered source. Further, the losing USACIDC will deactivate the registered source file upon departure and furnish all required documentation to the gaining unit. The gaining unit will initiate required documentation for the registration of the source upon arrival, making reference to the former registered source number.

(5) Where the registered source is not to be used by the USACIDC upon his arrival at the new duty station as designated by TAPC, no consideration for a specific unit of assignment will be made.

(6) When a specific unit of assignment is obtained by the USACIDC through coordination with the Special Actions Branch (SAB), TAPC, all possible measures will be implemented to prevent an immediate recurring FOL situation.

(7) In all instances where a source is moved on a FOL basis and elects to assist the USACIDC upon arrival at his new duty assignment, measures must be taken when using this individual to prevent an immediate recurring FOL situation. Individuals, as identified above, may be used in a capacity to develop information and report to USACIDC on those involved, thereby precluding the necessity for court testimony in most instances, and maintaining the covert status of the source.

(8) The SRO will evaluate the request for transfer on a FOL transfer. The SRO may require additional substantiating information to verify the FOL situation. Upon approval of the request for a FOL transfer, the SRO will coordinate with TAPC. The USACIDC field unit will not contact TAPC directly, unless the SRO is not readily available. Under normal circumstances, all coordination with TAPC will be accomplished through the SRO.

(9) Coordination with the gaining USACIDC unit will be implemented and is the responsibility of the losing USACIDC unit.

(10) The SCO at the requesting USACIDC unit will telephonically notify the USACIDC MSC when they have made a FOL transfer request to the SRO.

e. Threat Transfers (OCONUS).

(1) The appropriate USACIDC MSC will coordinate OCONUS to OCONUS FOL transfers with local servicing personnel centers. OCONUS to CONUS transfers will be coordinated with the MACOM theater staff element. When a situation cannot be resolved at that level, coordination may then be made with the SRO, who will coordinate with TAPC.

(2) All other FOL transfers will be coordinated IAW paragraph 14-10d above.

f. Sources who have received FOL transfers may be required to return to their former installations to testify at a later date. Disclosure at trial or at a pretrial hearing of the source's present duty station may place the source's safety in jeopardy, thereby requiring an additional FOL transfer. To avoid unnecessary expense and administrative inconvenience, coordination must be made with the appropriate trial counsel to ensure that such disclosure will not occur unless it is absolutely essential to judicial proceedings. Consideration should be given to providing the judge with this information in chambers, when necessary. Trial counsel should be alerted to the necessity of immediately informing the USACIDC of any such disclosure that does take place so that appropriate action may be taken to safeguard the source. In instances where a source returns to testify at a civil trial, coordination must be made with appropriate civil authorities to have the source's present unit of assignment deleted from testimony given in open court. Consideration should be given to providing the presiding judge with this information in chambers when necessary to negate the possibility of a recurring FOL situation. In all instances where a source, having received a previous FOL transfer, returns to testify at a military or civil proceeding, the USACIDC will provide adequate safeguards to ensure the source's safety or coordinate with civil authorities to ensure that this is accomplished.

g. Threat transfer of USACIDC personnel.

(1) For the purpose of this chapter, “USACIDC personnel” are defined as all personnel assigned to CID and MPs, and MPIs when involved in USACIDC operations, and their family members. MP/MPI threat transfers will be handled in coordination with their respective chain of command.

(2) When a CID supervisor confirms that there is a credible threat to the safety of USACIDC personnel and a transfer from the installation is deemed necessary to assure their protection, the following procedures will be followed:

(a) The threat will be reported through the chain of command to the USACIDC MSC. The commander will evaluate the threat and make the determination as to whether or not there is a clear and present danger to USACIDC personnel and their family.

(b) In the event that the USACIDC MSC determines that a FOL transfer is warranted, he/she will notify the USACIDC DCSOPS. The MSC will also notify the initiating USACIDC unit and advise them of the notification to HQUSACIDC. Coordination will be made between the DCSOPS and the DCSSPT to obtain a list of suitable new assignments.

(c) The SRO will be provided the relevant facts and circumstances pertaining to the action along with the date and time transfer was approved by the USACIDC MSC. The SRO will obtain the USACIDC person's new assignment

from TAPC and then notify the DCSOPS, DCSSPT, and the initiating USACIDC unit. If a civilian CID agent is involved in a FOL situation, the civilian agent will be reassigned by HQUSACIDC.

(d) If the FOL transfer involves a MP or MPI, coordination will be made with the service member's unit commander prior to coordination with the SRO.

(e) The initiating USACIDC unit will transmit by message the synopsis of the events necessitating the transfer to the gaining USACIDC MSC and gaining USACIDC unit.

14-11
Discontinued Use of Registered Sources

a. When the source handler determines that the services of a source are no longer desirable, or the source is locally deactivated for any reason, the file will be placed in an inactive status and destroyed in accordance with AR 25-400-2. An entry reflecting the basis for the source's deactivation will be placed in the source file. Deactivation is a triggering event. Notification to the SRO will be accomplished by sending one copy of the source's data card reflecting the date and reason for deactivation, to CDR, USACIDC, ATTN: CIOP-IN-SRO. The mailing procedures established in this chapter will be followed.

b. A debriefing will normally be conducted when the source is no longer providing information. The results of the debriefing will be annotated in the source file. During the source debriefing, it should be emphasized that it is to the source's advantage that the assistance he rendered to the USACIDC and to the Army be kept confidential. The source will also be advised that, although formal assistance to the USACIDC is no longer required, the local USACIDC unit should be notified of any threats which may be directed toward him as a result of services previously rendered. The CID agent conducting the debriefing should attempt to obtain any criminal intelligence known to the source and not previously provided to the USACIDC.

c. If debriefing a registered source is not considered appropriate in the judgment of the handling agent and/or SCO, an entry to this effect will be included in the source file, explaining the specific circumstances.

14-12
Restrictions Governing Information Collection

a. Sources are usually not law enforcement personnel and may be unfamiliar with restrictions as to the type of information USACIDC may legally collect. As a result, CID agents must ensure that information collected by a source has a

military connection and is pertinent to the law enforcement functions of the USACIDC.

b. The USACIDC may receive and record only that data which is consistent with the USACIDC investigative mission. Files may contain only that information on persons and/or organizations which clearly connects them to matters affecting legitimate military interests. Information gained incidentally, while in pursuit of an investigation within the USACIDC mission, which relates to crime in another jurisdiction will be referred to the appropriate agency as soon as possible.

c. USACIDC supervisors will ensure an evaluation is made upon initial receipt of any information from sources to verify that its retention is appropriate. Further evaluation will be accomplished whenever additional information alters the character of the initial report.

d. Under the provisions of AR 340-21, information from sources concerning purely political activities or personalities, in which no criminal activity is indicated or suggested, will not be collected, recorded or reported.

14-13
General

a. A system of recording certain information and maintaining specific files is necessary to ensure that source related efforts are coordinated, that sources and their handlers are protected, and that the information obtained from sources is put to the most efficient possible use. A record system for each source concerning the source's activities and biographical information will be maintained by the USACIDC. All files will be maintained IAW AR 25-400-2, under file number 195-2g. Receipts from registered sources will be maintained in the individual source file. Receipts from open sources will be maintained in the appropriate case file. In addition to those files specified in AR 25-400-2, the following files will be retained under that file number as "other documents" when needed.

(1) Incoming correspondence. This file will include, but is not limited to, material from the SRO and SCOs. The file is for source information only and not for general office correspondence.

(2) Outgoing correspondence file. This file will include, but is not limited to, letters to the SRO and SCOs about sources. The file will not be a general correspondence file for non-source material.

(3) Miscellaneous file. This file is for internal office memos, MFRs, notes on quarterly inventory/review files, and general office correspondence.

(4) Source transfer file. This file is for correspondence received from a USACIDC unit transferring a source who has PCS'd and has shown a willingness to continue work as a USACIDC source.

b. The files will be maintained on a calendar year basis and retained in accordance with AR 25-400-2.

c. Due to the nature of source operations, only the most essential records of source activities and related files will be sanctioned and established.

14-14
The USACIDC Central Source Register

The CSR is a legacy file system which allows the USACIDC to identify former registered sources, assist in FOL transfers, and collect information related to registered source usage. It will be maintained by the SRO. This register will consist of source data cards forwarded from USACIDC field unit to the SRO.

a. Access to the CSR by anyone other than the SRO will be authorized only by the CG, USACIDC or the DCSOPS, USACIDC.

b. The SRO is responsible for protecting the contents of the CSR from unauthorized disclosure. This register contains extremely sensitive information and will be safeguarded at all times. It will be stored only in an approved security container. If the register is removed from this container, the register will be under constant observation and protected from compromise.

c. A source data card is the means of recording information in the CSR. It will be completed on each registered source by either the SCO or the source handler following recruitment of the source.

(1) Figure 14-1 contains specific guidance for preparation and use of the source data card (CID Form 20).

(2) Identification and background information on the source data card is highly sensitive. Appropriate discretion should be used in acquiring and using this data. Sources may be reluctant to divulge needed information. Every effort will be made to fully complete this form; however, partial completion is authorized in specific instances when using unwitting sources. Unwitting sources may fall into different categories. One could involve a person who, without knowing the true identity of the agent, provides information to the agent. Another unwitting source might be a person who voluntarily gives information, over an extended period, to an overt agent, but may stop providing information if exposed to the formal registration process. In these instances, the source data card should be completed as fully as possible using indirect methods of questioning or through

review of related public or administrative records. Extreme care should be exercised to avoid compromise of the source when record review methods are used. When a source data card is partially completed, annotate the form with the term "Unwitting Source." Appendix M contains a complete guide to source management and should be consulted for further details and source management procedures.

(3) A photograph of the source may be included in the source file at the discretion of the handler and SCO. Such photographs may be obtained directly from a source, through existing facilities with the source's consent, or by covert means without the source's knowledge. Source photographs do not follow any specific format. Source photographs of minors will only be exposed upon the specific written consent of the minor’s parent(s) or guardian(s).

(4) Prior to requiring the source's social security number (SSN), USACIDC agents must notify the source that:

(a) The SSN is requested under authority of 10 USC 3012g and 5 USC 301, and

(b) that the SSN will only be used to aid in identification by the handler and

(c) that the source may voluntarily furnish the SSN or it may be obtained from official records.

(5) Upon a triggering event, the original source data card will be placed in a sealed envelope and marked “SRO EYES ONLY.” This envelope will then be transmitted by certified mail, return receipt requested, CDR, USACIDC, ATTN: CIOP-IN-SRO. A DA Form 209 and/or DA Form 4510 may be used if, in the opinion of the handler or SCO, additional mail control procedures are required. When the situation warrants, more than one source data card may be placed within one envelope and mailed. When the original source data card is mailed to the SRO, a copy of the form will be maintained in the individual source file.

14-15
USACIDC Unit Source Files

Active and inactive individual register files, registered source ledger, and the other administrative files pertaining to sources will be consolidated in a secured container with limited access.

a. The individual registered source file will consist of a manila folder, marked with the registered source number and the appropriate MARKS label. The folder may be marked in some manner to make it conspicuous. The folder will contain a

source data card and any other documents deemed appropriate by the handler or SCO (receipts, statements, Declaration of Understanding, AAS, etc).

(1) Details of source activities during the course of an investigation, which will be documented by a ROI, CPS or CIR, will be documented either on the AAS within the individual case file, the ROI, or AIR within the case file.

(a) The AAS within a source file will be used to describe details of meetings and source activities which are judged by the handler as not having value to the eventual resolution or prosecution of an investigation, or which may present a security risk to the source if recorded in a regular case file. Information not considered appropriate for external publishing might include meetings to reimburse expenses of a source or to discuss security measures regarding the source's identity or safety.

(b) If a source's activity has a direct investigative bearing on an ongoing case, the details of such activity should be documented in the case file and associated final ROI.

(c) A MFR may be used within the source file to document information of a sensitive nature of interest only within USACIDC channels, such as aspects of the source's conduct.

(d) Registered sources will be referred to by source code number on the AAS and MFR (when used in the manner described above). When source activities are discussed in final reports (ROI, CIR, CPS, or AIR), the source will be referred to as "a source," or a "CID source," but not by number or name. If more than one source's activities apply to the same case, they should be referred to in final reports as, "CID source," "source 1," "source 2," and so forth. The source code number will be recorded in the AAS in a case file as a means of cross referencing.

(2) Receipts obtained from registered sources will be retained in the individual source file folder.

(3) Source files may contain other documents deemed appropriate by the local USACIDC supervisor and/or SCO.

b. Normally, a source file will be maintained at the USACIDC unit using the source. If sources are used by USACIDC units not responsible for maintaining case files, their source files will normally be maintained by the SCO at the USACIDC field unit which is maintaining those files. If the SCO is not co-located with the source handler, as may be the case where a drug suppression team is maintaining office space in a safe-house or elsewhere, the source handler may maintain his own source files and place a “skeleton folder” in the SCO files bearing the source number(s) and referencing the actual location of the file. The

SCO, in such cases, will continue to monitor the files and activities of these sources.

c. Source files will be stored in a locked file cabinet or safe and access will be restricted to the SCO, source handlers for their individual source files, team chief, and supervisory personnel. A USACIDC MSC may authorize certain members of the staff to have access to the source files of subordinate units for inspection purposes. The USACIDC Inspector General is authorized full access to all source files and information.

14-16
Source Code Number

a. Each registered source will be assigned a code number by the USACIDC unit to which the source provides information. These numbers will be entered on the source data card. The registered source number will consist of two groups of digital information preceded by the letters “RS” as follows:

(1) The USACIDC unit number. This is the number of the USACIDC unit using and registering the source.

(2) Source number. This is a four-digit number assigned by the USACIDC unit SCO. For example, RS014-0001 identifies the source file as being the first source recruited by the Fort Bliss CID. Source numbers will continue to be issued consecutively, having begun with 0001 and running through 9999. If there is a need for additional numbers, revert to 0001 and the suffix "A," then use 0001A through 9999A. The next higher letter in the alphabet will be used each time the numerical designation of 9999 is surpassed.

(3) The registered source ledger will be a bound book. The ledger will be sequentially numbered for the registered source number and contain the source's name, social security number, unit or location, handler and agent's sequence number, date recruited and terminated, and remarks. See Figure 14-6 for an example.

b. After a registered source code number has been assigned, all internal USACIDC correspondence referring to that source will be by the source's code number.

c. The registered ledger books will be permanent documents.

14-17
Source Data Card

A separate source data card will be completed for each registered source (Figure 14-1). When a triggering event occurs, the original card will be forwarded to SRO and a copy will be maintained in the individual source file.

CHAPTER 15

15-1
Purpose

This chapter prescribes policies and procedures to be used in the performance of the USACIDC protective services mission.

15-2
Definitions

See page 132, FC 19-136, Protective Services.

15-3
Authority and responsibility

a. AR 10-87 assigns the Commanding General (CG), USACIDC, the function of planning and conducting protective service operations involving individuals designated by higher authority. Primary focus is placed upon the protection of the Secretary and Deputy Secretary of Defense; Chairman and Vice Chairman of the Joint Chiefs of Staff; Secretary of the Army; Chief and Vice Chief of Staff, U.S. Army; and their foreign counterparts when visiting the United States as official guests of the U.S. Government. Unless otherwise directed, such missions remain under the operational control of the CG, USACIDC.

b. According to the provisions of AR 190-58, the protection of dignitaries other than those outlined in paragraph 15-3a above is normally the responsibility of the commander exercising jurisdiction over the area visited. When requested and consistent with operational priorities, USACIDC subordinate elements will support local commanders providing the protection. Such support will be documented according to other parts of this regulation.

c. Other responsibilities

(1) Commander, Investigative Services Activity (ISA), USACIDC: Responsible to the CG, USACIDC, for supervision of the Protective Services Unit (PSU), an operational element of the ISA, and monitorship of the overall USACIDC protective services function. In this regard, he exercises authority to task USACIDC major subordinate commands for support necessary to accomplish the mission. The Deputy Chief of Staff for Operations, HQUSACIDC, will be informed of all such taskings to USACIDC major subordinate commands.

(2) Deputy Chief of Staff for Operations, HQUSACIDC: Will exercise operational oversight of all taskings to USACIDC major subordinate commands

to ensure an equitable allocation of resources, that criminal investigative operations are not impeded, and will arbitrate disputes over taskings.

(3) Deputy Chief of Staff for Support, HQUSACIDC: In close coordination with the Deputy Chief of Staff for Operations and the U.S. Total Army Personnel Command (PERSCOM) ensures qualified agent replacements are assigned as required.

(4) Commander, PSU: Plan, manage, super-vise and execute all PSU missions assigned directly to and under the operational control of HQUSACIDC.

(5) USACIDC Major Subordinate Commands

(a) Ensure a representative at each applicable USACIDC major subordinate command is designated to act as coordinator of protective service operations with the PSU, subordinate elements and other supporting agencies.

(b) Establish and maintain close liaison with local military and civilian law enforcement/intelligence agencies to facilitate the collection of any information that could adversely affect the security of DoD officials.

15-4
Policy

Commanders and individuals at all levels of command are responsible for complying with the contents of this regulation. The application of principles, methods, and techniques contained in Field Circular (FC) 19-136, Protective Services , will be closely adhered to when implementing this chapter.

15-5
Support to government agencies

a. General. Statutes and regulations authorize the USACIDC to provide protective services support to the U.S. Secret Service, Department of State and Department of Defense (DoD) in accomplishing their protective duties. (See FC 19-136 for the relevant statutes and regulations.)

b. Concept of operation

(1) Requests from DoD and DA elements for protective services support will be forwarded in writing through the Director of the Army Staff (DAS), Office of the Chief of Staff, Army to the Deputy Chief of Staff for Operations and Plans (DCSOPS) for approval. The DCSOPS will task USACIDC for security/support requirements. Requests from agencies outside DoD (except the U.S. Secret

Service) will be forwarded by USACIDC through DCSOPS to the DAS for a decision on whether the support will be provided by USACIDC. Requests from the U.S. Secret Service will be handled in accordance with AR 1-4.

(2) Upon notification of an impending protective services mission, CID action procedures in accordance with this regulation, and FC 19-136 will be followed.

(3) The PSU will determine the degree or level of security for the mission based upon the conduct of a threat assessment and the following factors:

(a) Threat Level (general area and specific) - low, medium, and high.

(b) Location (CONUS vs. OCONUS, military installation vs. civilian community).

(c) Principal.

(d) Duration of mission.

(e) Type of quarters when the principal remains overnight (i.e., private, ambassador's residence, commercial hotel).

(f) Nature of public exposure (required by circumstances and/or desired by principal).

(g) Local/host government police support (level and type of support).

(h) Ideologies of the population visited.

(i) Modes of transportation to be utilized.

15-6
Selection, training and conduct

a. Selection criteria. Special agents selected for assignment to PSU will meet the following minimum standards:

(1) As established by AR 195-3.

(2) Weight control standards according to AR 600-9.

(3) The Army physical fitness test according to FM 21-20.

b. Desirable Traits. Special agents selected for assignment to PSU must be in excellent physical and mental condition, of established reliability, presentable in

appearance, intelligent, articulate and capable of making instinctively correct decisions in emergency situations. These qualifications are very subjective. The following desirable traits of a PSU agent are listed for reference by supervisors at all levels when considering an agent for assignment to PSU.

(1) Judgment. Foremost among the desirable traits for a PSU agent is the ability to consistently exercise sound judgment even under stressful and rapidly changing situations. The well being of the principal may needlessly be placed in jeopardy or his image discredited by an error in judgment by the assigned PSU agent at a critical moment. Any history of poor judgment must be examined closely when considering an agent for an assignment to PSU. The PSU is a uniquely stressful assignment and will place demands upon an agent not encountered in any other USACIDC assignment. If the agent's judgment has been called into question in less stressful and demanding situations, it is unwise, and unfair to the agent, the command, and the principals he may be assigned to protect to place the agent in a position where an error in judgment might well be fatal. Decision making may be taught and may improve with experience; whereas judgment is a basic quality which is usually developed by the time an individual becomes an agent.

(2) Experience. Agents selected for PSU assignment should be senior journeyman agents with a wide range of experience. By the nature of their mission, PSU agents are in continuous direct contact with senior DoD officials and their foreign counterparts. The PSU agent must work directly with aides-de-camps, senior military aides, and other high ranking staff members supporting the principal.

(3) Maturity. Agents selected for assignment to PSU should have demonstrated the professional maturity to work without supervision, praise, or reward. The PSU agent may work 18-20 hours a day for a principal who may give the agent little or no recognition. Agents easily offended or given to feeling slighted by a lack of praise or even personal consideration is not suited for the psychological stress of protective service duties.

(4) Demeanor. The PSU agent must possess the demeanor to establish a cordial yet professional working relationship with personnel of all grades and positions. The agent cannot be intimidated by flag officers or overbearing toward military police personnel or drivers assigned to support the principal. The PSU agent must be able to function properly dressed in BDUs at a field training site or in black tie at a formal dinner given by a head of state. He/she must maintain a cordial y et detached professional relationship with the principal, his family and staff in the face of friendly overtures or hostilities. The PSU agent must be knowledgeable of protocol procedures and possess the flexibility to accept the customs of the many countries in which he/she will work.

(5) Mental Fitness. The PSU agent must be mentally sharp. He/she must be able to block out all personal considerations from the mind and concentrate on the mission for long tedious hours. Agents who do not possess the inclination or stamina to work 18-20 hours a day for extended periods will find protective service missions excessively taxing, both mentally and physically. The combination of vast responsibilities and a rapidly changing environment creates an extremely stressful situation for the PSU agent. This stress will continue indefinitely for the entire duration of the mission. Only agents who have demonstrated they can effectively deal with great stress should be considered for a PSU assignment.

(6) Physical Fitness. During a protective services mission, many hours of travel via assorted modes of transportation and prolonged walking and standing will draw heavily on the stamina of a PSU agent. The ability to achieve a certain score, even the maximum score, on the APFT will not ensure that an agent can endure the prolonged stress of a PSU mission. Constant travel throughout the world will disturb sleep patterns, dietary norms, and exercise routines; yet after many 18-20 h our days the PSU agent must be capable of swift reaction to a threat to his/her principal. PSU candidates must be physically fit and adaptable to changing environments.

(7) Tact. At each location visited by a principal, there is a host. The host may be an installation commander, a senior State Department official, or a host country officer or official. Many times there are several hosts, each with their own goals for the visit. Often the host(s) will have spent months planning for the principal's visit. The host may not have considered security at all in the planning or he will have tried to orchestrate the visit from both a security and protocol standpoint. Either way, the PSU agent must coordinate security arrangements with the host and many times is placed in the position of having to recommend or direct changes. It is imperative that the PSU agent exercise great tact in making the recommendations for change as his/her handling of the situation may reflect upon the principal. Tactfulness should not be confused with weakness or acquiescence. Since the PSU agent is ultimately responsible for the security of his/her principal, the agent must be decisive while concurrently demonstrating great tact in coordinating the change with the host.

(8) Decisiveness. The PSU agent is called upon to make a number of decisions during the course of each protective services mission. Those decisions required prior to the arrival of the principal at the location to be visited normally need not be made instantaneously and there is sufficient time for deliberation. However, many of the decisions required during the actual period of the principal's visit must be instantaneous and made with little or no deliberation. Indecision on the part of the PSU agent may result in embarrassment or actual harm to the principal. Further, once the agent has made a decision, he/she must be prepared to follow through with that decision.

(9) Assertiveness. The PSU agent is ultimately responsible for the security of the principal he/she is tasked to protect. To make and implement decisions which may be opposed by officials far senior to the agent. In making a decision, the agent must draw upon his/her judgment, experience, maturity, and decisiveness. When certain of his/her decision, the agent must make maximum use of his/her demeanor and tact in articulating the reasoning which supports his/her decision to overcome opposition. However, because of his/her responsibility to the principal, the PSU agent must be prepared to assert himself/herself when diplomacy, compromise, and reason fail.

(10) Communicative skills. The PSU agent must be an effective communicator. He/she will be required to communicate with personnel at all levels of the military and diplomatic corps, both foreign and domestic. The PSU agent must be able to articulate security requirements with professional confidence without appearing to be overbearing. The success of a protective services mission is dependent upon the support and cooperation of many individuals and agencies. That support and cooperation is more effective when freely given based upon a cordial, professional relationship with the PSU agent rather than begrudgingly given because of the principal's position. Effective communications also requires that the PSU agent be skilled in listening as well as articulation.

(11) Flexibility. The planning of a protective services mission begins with the principal's itinerary. The itinerary will undergo change during each phase of preparation for the visit and each change will affect security. The agent must plan beyond the scope of the itinerary. Contingencies for each aspect of the visit must be considered prior to the principal's arrival and a plan devised for each contingency. In spite of exhaustive planning and preparation, unforeseen changes will occur during the principal's visit and the agent must be flexible enough to immediately adjust the entire security posture.

(12) Adaptability. The PSU agent must be capable of adapting to radical changes in culture and procedures. The principals whom the agent will be tasked to protect travel extensively and the agent may be working in the Middle East, the Orient, and Europe in the same week. Each country and region will have different customs, languages, and security methods. The agent must be adaptable to provide the principal effective protection without offending the host country agencies with who m he must work. Even when conducting protective service operations in the United States, the PSU agent will be confronted by officials with different perceptions of security requirements. Whenever consistent with acceptable security practice, the agent must be prepared to compromise and adapt his/her method of operation to accommodate the desires of the principal and/or his/her host. Judgment must be used to balance between assertiveness and adaptability.

(13) Dedication. The PSU agent may be tasked to protect an individual who represents a political orientation with which the agent does not agree or possibly a government hostile to the United States. The PSU agent must be prepared to give every principal he/she is tasked to protect the same quality service and, if necessary, give his/her life to protect the principal. The PSU requires the ultimate dedication.

c. Training

(1) Prospective PSU agents will attend the Protective Services Training Course at the Military Police School en route to their permanent change of station to PSU, unless the training was accomplished at an earlier date.

(2) When possible, prospective PSU agents will attend anti-terrorism/evasive driver training en route to their permanent change of station to PSU; otherwise, agents will be programmed to receive this training as soon as possible following their assignment to PSU.

(3) Upon assignment to PSU, agents will meet, at a minimum, the following qualifications:

(a) Be trained in the use of assigned weapons (9mm pistol; 12 gauge shotgun; machine pistol) and will have qualified in accordance with chapter 17 of this regulation. Failure to maintain proficiency and qualification will subject personnel to reassignment.

(b) Be certified or re-certified in cardiopulmonary resuscitation techniques.

(4) Upon assignment to PSU, agents will undergo approximately six to nine months of intensive on- the-job training in protective service operations.

(a) Agents will become proficient in the operation and use of specialized equipment (e.g., communications, electronic surveillance, police emergency equipment, etc.).

(b) Agents will hone executive protection skills and techniques.

d. Conduct. PSU members will maintain unquestionably proper standards of conduct. This includes:

(1) Abstaining from consuming any alcoholic beverage 12 hours prior to and during the execution phase of the mission.

(2) Conforming to protocol procedures.

(3) Tactfully refusing gifts or favors from the principal or the official party, unless the refusal would offend them. Any gift or favor accepted will be immediately referred to the Commander, PSU, for proper guidance and/or disposition according to AR 600-50 and AR 672-5-1.

(4) Keeping all contacts with the principal, his staff and family on a formal basis. Agents will not attempt to enter into personal relationships with these parties.

e. Termination. Violations of or failure to meet or attain any of the provisions set forth may provide cause for termination of assignment to protective service duties or necessitate other administrative or punitive action considered appropriate by the CG, USACIDC, or his designee.

f. Protective services support

(1) Protective services support requiring additional special agent personnel will be tasked by the Commander, PSU, through the respective USACIDC major subordinate command, to assist in providing close-in personal security at specific locations to be visited by the principal. Only CID special agents and apprentice agents who meet the requirements of a(2) and (3) above and are qualified with their assigned weapon according to chapter 17 of this regulation, may be utilized for the close-in protective detail and control room operations. battalion commanders may approve assignment of apprentice agents to PSU operations subject to the following criteria: successful completion of at least 6 months of the normal 12 month apprentice period, or 3 months with the completion of the U.S. Army Military Police School (USAMPS) Protective Service Training (PST) course. Successful is defined as satisfactory performance in a field element as evaluated by the supervisor and unit commander or special agent-in-charge, in accordance with CID Pamphlet 195-5. The Commander, PSU, can request, on a case-by-case basis, that only accredited special agents be assigned to selective PSU support operations due to the nature of the operation and/or the status of the principal. Utilization of non-special agent personnel requires approval from the Commander, PSU. Non-special agent personnel (i.e., commissioned officers, military police and military police investigators) are normally utilized for the second or middle ring of security and not for the close-in protective detail or control room operations. Agents assigned to support PSU operations will become familiar with the control room operation procedures as depicted in the sample at appendix N.

(2) When the mission site is in a geographical area where the Air Force Office of Special Investigations or the Naval Criminal Investigative Service have a field element, and USACIDC does not, PSU will coordinate protective service s support from those organizations through their respective Protective Services Program Manager. Should the mission occur in a geographical area where more

than one military criminal investigative organization has a field element, PSU will coordinate splitting the tasking among those organizations.

(3) The procedures outlined in paragraph 15-9 will be followed when PSU disseminates projected taskings for protective services support.

15-7
Funding

a. The HQUSACIDC will program funds to provide protective services support to the Chairman and Vice Chairman of the Joint Chiefs of Staff, Secretary of the Army, Chief and Vice Chief of Staff, Army, and any other principals as directed by the CG, USACIDC. The Commander, ISA will budget for funding requirements based on prior year expenditures and known and potential missions. To permit accurate programming and budgeting of funds, the Commander, ISA, will also maintain a record of al l actual expenditures for DoD and U.S. Army missions, to include accounting for DoD missions that were directed to be funded by HQUSACIDC.

b. Protective service missions in support of the Secretary and Deputy Secretary of Defense, and other missions designated by higher authority, will normally be funded by the Office of the Secretary of Defense or the requesting agency.

c. Members of the PSU and field agents traveling with the principal will be reimbursed for travel expenses using the following procedures:

(1) Actual expense allowance authorization for PSU travel will be requested by the PSU quarterly through command channels from the Commander, USACIDC, ATTN: CISP-RM-PB, in accordance with the procedures contained in Joint Federal Travel Regulation, Volume I.

(2) All other mission-related expenditures will be reported in accordance with AR 195-4.

15-8
Operational reporting

a. Field elements. When information is developed or received by field elements that may affect the security or safety of any principal for whom the CG, USACIDC, is charged with protecting, that information will be transmitted immediately to the Commander, PSU, ATTN: CISAP-OP, by the most expeditious means available. Telephonic notification may be appropriate if the information is time sensitive. A copy of other threat information will be forwarded by routine means to the Commander, PSU , ATTN: CISAP-OP.

b. PSU. The preparation, advance, execution, and post mission phases involved in a protective services mission will be reported according to the procedures, records, and forms used in accordance with PSU standard operating procedures.

15-9
PSU monthly field agent tasking

a. Each month PSU will disseminate projected field agent requirements in support of all PSU missions forecasted for the following month. Dissemination will be in writing (figure 15-1) to all USACIDC major subordinate command protective service coordinators and the protective services program managers for the AFOSI and NCIS.

b. The information below serves as a reference guide for interpreting the tasker so that its content may be kept brief and eliminate redundancy.

c. The principal's identity will be reflected under the column labeled "PRIN" using the following numerical code.

1 Secretary of Defense (SECDEF)

2 Deputy Secretary of Defense (DEPSECDEF)

3 Chairman, Joint Chiefs of Staff (CJCS)

4 Vice Chairman, Joint Chiefs of Staff (VCJCS)

5 Secretary of the Army (SECARMY)

6 Chief of Staff, Army (CSA)

7Vice Chief of Staff, Army (VCSA)

8 SECDEF/CJCS Foreign Counterparts

9 CSA Foreign Counterparts

d. For principals in the eight and nine category their official title and position will be reflected one-time in the tasking document.

e. The column labeled "DATES" will relate only to the date(s) the principal will be on site, not the advance time.

f. The column labeled "SEQ" will reflect only the first four digits of the mission sequence number in lieu of repeating the entire sequence number (XXXX-02-CID011).

g. The column labeled "MSAC" will reflect the last name of the mission special agent-in-charge. However, addressees must keep in mind that assignments sometimes change after the monthly tasking document is dispatched.

h. Agent availability date. Unless notified otherwise by PSU, support agents will be available on-site one full day prior to the start of the principal's visit. This will allow time for briefings, assignment instructions, route and site reconnaissance, and etc. Therefore, those who must fly in or otherwise travel long distances, should arrive on-site no later than 1800 on the evening prior to their availability date. This will enable the agent to check into the hotel and get a good night sleep before beginning work.

i. The PSU personnel will make lodging accommodations and as soon as possible they will telephonically furnish information to the USACIDC major subordinate command designated point of contact concerning lodging, arrival instructions, plus time and place for agents to meet the PSU advance team.

j. Identification data. Addressees will identify agents as soon as possible and furnish the following information to PSU: name, rank, SSAN, unit of assignment, security clearance, and as applicable, flight itinerary, passport number/place of issue/issue date/expiration date, DOB/POB, and weapon type/caliber/serial number.

k. When support agents will travel into a foreign country, USACIDC major subordinate command protective services coordinators will include the appropriate U.S. Embassy //DAO// AND //RSO// as info addressees on any messages sent to PSU concerning the information in paragraph j. above.

l. Information on visa requirements, weapon transport restrictions/prohibitions, or special equipment requirements (i.e., protective vests), will be specified in the tasking document.

m. Fund cite information

(1) For missions involving principals one or two, OSD fund cites will be disseminated in writing by PSU to the USACIDC major subordinate command protective service coordinator after the agent data in paragraph j above is furnished to PSU. Travel order numbers will be issued by name and substitutions are not authorized.

(2) For missions involving all other principals, USACIDC funds cites will be used for CID support agents.

n. Special instructions for TDY orders

(1) Authorization for rental vehicles.

(2) Authorization for taxi fares.

(3) Upon receipt of paid settlement voucher from finance, a legible copy of the travel order and settlement voucher will be forwarded to Protective Services Unit, USACIDC-ISA, ATTN: CIS, Building 2223, Fort Belvoir, VA 22060-5353.

15-10
Protective service security control room standard operating procedures

a. Purpose. To ensure uniformity and continuity of effort for security control room standard operating procedures (SOP).

b. Procedures

(1) This SOP (appendix N) will be utilized for all PSU missions where a control room is established.

(2) Mission special agent-in-charge (MSAC) will thoroughly brief all agents supporting the mission on the contents of the SOP and its enclosures. All agents supporting the mission will read the SOP with enclosures and attest to the fact that they have been briefed, read, and understand its contents by signing the certification page at the back of the SOP.

(3) The MSAC will post the signed certification sheet (less the SOP itself) in the respective mission file following mission completion.

CHAPTER 16

16-1
General

The USACIDC Combating Terrorism Program is governed by AR 525-13, The Army Combating Terrorism Program. The program is designed to collect, process and disseminate criminal intelligence and information pertaining to terrorism within USACIDC and to affected commanders. It also ensures that the information gathered through collection is properly acquired, retained, and disseminated as directed by DoD/DA.

16-2
Purpose

This chapter establishes basic USACIDC guidance for the conduct and management of the USACIDC Combating Terrorism Program. It de-fines responsibilities for personnel implementing the program. It further prescribes procedures for the collection, processing, and dissemination of criminal information pertaining to terrorism within USACIDC and to affected commanders.

16-3
Scope

This chapter provides guidance to HQUSACIDC staff and subordinate USACIDC elements, and applies to all assigned or attached personnel at all levels of the command.

16-4
U.S. Government and Army Policy for Combating Terrorism (Extracted from AR 525-13)

The U.S. position on terrorism is unequivocal: firm opposition to terrorism in all its forms wherever it takes place. The U.S. Government is strongly opposed to domestic and international terrorism; considers the practice of terrorism by any person or group a potential threat to national security; and will resist acts of terrorism by all legal means available. The U.S. Government will make no concessions to terrorists and will respond aggressively to terrorist acts without surrendering basic freedoms or undermining democratic principles.

16-5
The Army Combating Terrorism Program (CBT/T) responsibilities assigned to the USACIDC

a. Collect, evaluate, and disseminate to affected commands criminal information pertaining to terrorist activities, within the provisions of applicable statutes and regulations.

b. Provide terrorist related criminal information to HQDA (ATOIC), the U.S. Army Intelligence and Security Command (INSCOM) and the U.S. Army Intelligence and Threat Analysis Center (USAITAC).

c. Investigate terrorist incidents on installations and facilities, and against units, Army personnel, or their family members. Monitor the conduct of such investigations when conducted by civilian or host nation police agencies. Provide results of terrorism related investigations to HQDA (ATOIC) and the Center for Army Lessons Learned (CALL).

d. Provide trained hostage negotiators to support Army CBT/T operations worldwide.

e. Plan and coordinate personal protective services for DoD and DA officials, as directed by HQDA.

f. Report terrorist incidents, suspected terrorist activity and criminal information concerning the terrorist threat to appropriate local commanders.

g . Serve as the Army's principal liaison representative to federal, state, and local law enforcement agencies to exchange terrorist-related criminal information.

h. Conduct personal security vulnerability assessments (PSVAs) for all personnel designated by MACOM commanders and other Level I high risk personnel (HRPs) as directed by HQDA. Provide technical assistance to local provost marshals during the conduct of PSVAs for Level II HRP.

i. Establish procedures to ensure appropriate liaison at all levels between USACIDC and INSCOM

16-6
Responsibilities

a. The Commanding General, USACIDC, through the Deputy Chief of Staff for Operations, will be responsible for:

(1) Providing the command and staff supervision of the USACIDC Combating Terrorism Program, ensuring that it is in compliance with AR 525-13.

(2) Appointing a headquarters combating terrorism officer to implement and oversee the program.

(3) Coordinating with federal law enforcement agencies, national intelligence agencies, major Army commands, and state and local law enforcement agencies, as appropriate, concerning information developed from CBT/T.

(4) Coordinating with the Director, Crime Records Center to process terrorism related criminal intelligence for an up-to-date centralized index for criminal information.

(5) Reevaluating the effectiveness of the Combating Terrorism Program and initiating improvements where necessary.

b. The HQUSACIDC combating terrorism officer will be responsible for:

(1) Managing and supervising the USACIDC Combating Terrorism Program in accordance with AR 525-13.

(2) Publishing policies, guidance, letters of instruction, and regulatory changes as required for the efficient management of the Combating Terrorism Program.

(3) Coordinating with criminal intelligence analysts at HQUSACIDC to ensure that criminal intelligence, as related to terrorism, is being collected, processed, and disseminated properly.

(4) Coordinating with USACIDC staff and field elements on criminal intelligence involving terrorist acts.

(5) Reevaluating the effectiveness of the Combating Terrorism Program and making improvements, where necessary.

c. The HQUSACIDC criminal intelligence analysts will be responsible for:

(1) Reviewing all Criminal Intelligence Reports (CIRs), selected Reports of Investigation (ROI), and other investigative reports for criminal intelligence involving terrorism.

(2) Recommending to the Deputy Chief of Staff for Operations, publication of criminal intelligence bulletins on items of terrorist criminal information deemed appropriate for command wide dissemination.

(3) Maintaining liaison with other federal service, and Army agencies for the purpose of exchanging criminal intelligence pertaining to terrorism.

(4) Coordinating with the HQUSACIDC combating terrorism officer on matters affecting the management and administration of the Combating Terrorism Program.

d. Commanders of USACIDC major subordinate commands, or their designated staff representatives, will be responsible for:

(1) Implementing and monitoring the Combating Terrorism Program throughout their area of responsibility in accordance with regulatory guidance.

(2) Coordinating terrorism criminal intelligence matters, as appropriate, with federal, state, and local law enforcement agencies operating within the major subordinate command's AOR.

(3) Coordinating with the supporting military intelligence units on matters concerning terrorism.

(4) Ensuring the establishment of a criminal intelligence element at each battalion, field office, and designated resident agency.

(5) Establishing a criminal intelligence element at the USACIDC major subordinate command for the coordination of all criminal information activities within their area of responsibility.

(6) Reevaluating the effectiveness of the Combating Terrorism Program within their area of responsibility and initiating improvements, where necessary.

e. The USACIDC major subordinate command's criminal intelligence investigator or coordinator will be responsible for:

(1) Reviewing CIRs received from subordinate elements for any criminal intelligence involving terrorism.

(2) Coordinating with the HQUSACIDC criminal intelligence and CBT/T officer on terrorist intelligence matters.

(3) Disseminating terrorist information/intelligence within their area of operation, as needed.

f. Commanders of USACIDC battalions/field offices will be responsible for:

(1) Implementing and supervising the Combating Terrorism Program in accordance with regulatory guidance.

(2) Ensuring that all assigned personnel are knowledgeable of the contents of this document.

(3) Coordinating criminal information matters as appropriate with federal, state and local law enforcement agencies operating within the battalion/field office area of responsibility (AOR).

(4) Coordinating criminal intelligence with local supporting military intelligence units.

(5) Ensuring terrorist related criminal intelligence is disseminated to the affected commanders.

g. The criminal intelligence investigator or coordinator at the battalion/field office and designated resident agency will be responsible for:

(1) Acting as the focal point for all criminal intelligence, identifying indicators of terrorist related pre-incident activities, and disseminating this intelligence to the affected commands, major subordinate command's headquarters and HQUSACIDC.

(2) In conjunction with the operations officer, reviewing selected investigative reports, collateral reports involving off post offenses normally investigated by CID, and other essential information for terrorist related criminal intelligence.

(3) Making available terrorist related criminal intelligence to agents during the initial and subsequent stages of investigations, inquiries, and other investigative actions.

(4) Coordinating terrorist related criminal intelligence with the local supporting military intelligence units.

h. Special agents will be responsible for the following in conformity with local procedure:

(1) Becoming familiar with the provisions of this regulation and understanding agent responsibilities inherent in the Combating Terrorism Program.

(2) Identifying and providing the criminal intelligence investigator or coordinator all criminal intelligence which could benefit the Combating Terrorism Program.

16-7
Investigate terrorist acts

a. Special agents will investigate all terrorist incidents directed against the U.S. Army, and will report the circumstances of the incident by the most expeditious means, regardless of who exercises primary investigative jurisdiction.

b. If either the FBI (CONUS) or host nation (OCONUS) authorities decline to assume jurisdiction, USACIDC will assume control of the crime scene at the earliest practical time.

16-8
Provide criminal intelligence related to terrorism

a. The USACIDC has the responsibility to collect, process, and disseminate criminal intelligence. Collection can come from sources, investigations, local, state, or federal police, military intelligence units, or host nation authorities.

b. Evaluation and dissemination of criminal intelligence on terrorist threats against U.S. Army installations, personnel, activities or property should be provided to the affected local commander, USACIDC major subordinate commands and HQUSACIDC. It should also be shared with the local supporting military intelligence units. Further dissemination requirements can be found in paragraphs 16-13 and 16-14.

c. The HQUSACIDC is responsible for conducting continuous coordination with federal law enforcement agencies at the national level to keep terrorism information updated and to analyze intelligence on a daily basis in support of the Protective Services Unit (PSU) mission.

d. The HQUSACIDC is also responsible for disseminating internally generated USACIDC terrorism information to the appropriate military and civilian intelligence agencies at the national level.

16-9
Provide hostage negotiators

a. The USACIDC provides trained hostage negotiators in strategic locations throughout the world.

b. The USACIDC primary and secondary negotiators must be identified based on their qualifications, experience, and training. When possible, USACIDC polygraph examiners should be identified as primary negotiators.

c. Identified negotiators should be used and trained with the supported installation's crisis reaction team/special reaction team (CRT/SRT). The negotiators will normally fall under the operational control of the installation or community provost marshal in a terrorist situation.

16-10
Conduct of Personal Security Vulnerability Assessments (PSVA) on Army Leaders.

a. A PSVA will be conducted for high-risk personnel upon their request, request of their staff, or when directed by higher authority.

b. High-risk personnel are designated in accordance with AR 525-13 and AR 190-58.

c. Personnel may be designated high risk based on assignment to a high-risk billet or based on personal factors, regardless of position. Examples of the former include senior general officers serving in prominent positions who could serve as symbolic targets for terrorist attack and U.S. military personnel of all ranks operating in areas where there is an active insurgency or frequent anti-U.S. violence. Examples of the latter include personnel who have established worldwide or regional prominence that transcends their position.

d. Through a PSVA, USACIDC assesses vulnerability to terrorist actions by addressing the current security posture, identifying weaknesses where they exist, and recommending corrective action.

e. Distribution of completed PSVAs will be made within 15 days for CONUS units and 30 days for OCONUS units.

(1) The original report with exhibits will be retained by the office conducting the PSVA.

(2) One copy with exhibits will be hand-carried and briefed to the PSVA subject or designated representative.

(3) One copy without exhibits will be sent to HQUSACIDC, ATTN: CIOP-IN, or e-mail ciopincps@belvoir.army.mil.

(4) PSVAs will normally not be classified. If a PSVA requires classification in accordance with reference 1a, it must be properly marked and packaged for dissemination. Classified PSVAs will be entered into ACIRS in accordance with paragraph 7-2 of CIDR 195-1. PSVAs previously classified warranting declassification must be accomplished in accordance with applicable regulations and guidance from the security manager, HQs, USACIDC.

(5) If not classified, PSVAs will be marked "Law Enforcement Sensitive", below the marking "For Official Use Only." The marking "Law Enforcement Sensitive" denotes sensitive law enforcement information discussing law enforcement techniques, operations, and risks not affecting national security. Furthermore, reports with this marking will only be released to third parties with a law

enforcement, force protection or security need to know. Release of the report must be approved by the special agent-in-charge. This marking will not be used on other CID reports until further guidance is published.

16-11
Personal security for senior Army leaders

a. Protective services by USACIDC are routinely provided to the Secretary and Deputy Secretary of Defense; Secretary of the Army; the Chairman and Vice Chairman, Joint Chiefs of Staff; the Chief and Vice Chief of Staff of the Army; and visiting foreign dignitaries and others when tasked by the Director of the Army Staff. Refer to Chapter 15 of this regulation.

b. The USACIDC PSU special agents are normally not provided to any other individual, except as an exception to Army policy, and only when approved by HQUSACIDC. However, technical advice on establishing protective services may be provided as priorities and resources permit.

c. Protective service operations are designed to safeguard a designated individual against assassination, kidnapping, injury, or embarrassment.

16-12
Planning considerations

When planning combating terrorism measures in coordination with supported installations, the following areas should be addressed:

a. Assess the vulnerability of USACIDC assets both on an installation and while deployed.

b. Integrate USACIDC preventive measures with the command or installation operations security and physical security plans.

c. Emphasize early warning of a potential terrorist incident through sound intelligence activities. This requires close coordination with local police agencies and supporting military intelligence units.

d. Establish close coordination with civil authorities and supporting military intelligence units to exchange information that indicates a threat to individuals or property on military installations and facilities.

e. Participate in installation contingency plans that will provide swift, effective reaction to bombings, assassinations and kidnappings. Address the use of USACIDC investigative and negotiator personnel. Stress to the command the

importance of developing and practicing a combating terrorism plan before a terrorist incident, to include the use of public affairs personnel, special reaction teams, negotiators, local law enforcement, etc.

16-13
Terrorist Incident Report (TIR)
(Extracted from AR 525-13 and modified for USACIDC use)

a. A TIR is used to report all terrorist and perpetrated incidents. Normal serious sensitive incident (SSI) format may be used.

b. When preparing a TIR, submit reports to the DCSOPS, ATTN: CIOP-ZA (normal duty hours) or the HQUSACIDC Staff Duty Officer (non-duty hours) by electrical message or telephone, priority precedence. A complete description of the terrorist incident will include the following:

(1) Type of incident and description.

(2) Location and description of incident site.

(3) Type of weapons used (bomb/firearm).

(4) Likely perpetrators.

(5) Claims of responsibility.

(6) Number of personnel injured and their condition.

c. When full details are known, the following additional information will be submitted:

(1) Possibly related terrorist threats or indicators prior to the incident.

(2) MACOM and other threat conditions (THREATCONS) prior to incident.

(3) Other anti-terrorism measures in effect prior to incident.

(4) U.S. and host nation actions taken (THREATCON) and changes/additional anti-terrorism measures in MACOM and locality since the incident.

(5) Any amplifying information available.

16-14
Terrorist Threat Report (TTR)
(Extracted from AR 525-13 and modified for USACIDC use)

a. A terrorist threat report is used to forward to HQUSACIDC any information available on terrorism or terrorist activity which might adversely affect the U.S. Army. The information may be unconfirmed. It may contain information of a general nature, or information on a specific threat.

b. When preparing a TTR, submit complete details to include the following:

(1) Individuals (if known) or groups.

(2) Usual modus operandi.

(3) Type of actions, weapons, or explosives normally used.

(4) Source of information and evaluation of the source.

(5) Evaluation of the validity of the information.

(6) Any amplifying information available.

c. In the case of an explicit threat against a U.S. Army specific or general target, include the following additional information if known:

(1) Likely perpetrators.

(2) Possible targets.

(3) U.S. (and host nation as appropriate) actions taken, if any (e.g., THREATCON changes, etc.) since receiving the threat.

(4) Any other amplifying information available.

d. Use a CID Form 97, Criminal Intelligence Report (CIR), for submitting a TTR containing information which is not time sensitive. If the information is on a specific threat in the near future, then an electronic message should be used.

CHAPTER 17

17-1
Purpose

This chapter establishes policy for carrying, using, safeguarding, and qualifying with weapons by personnel assigned to or under the operational control of USACIDC.

17-2
Responsibilities

a. The CG, USACIDC, is responsible for establishing policies for carrying, using, safeguarding and qualifying with weapons by individuals assigned to or under the operational control of USACIDC.

b. The USACIDC unit commanders at all levels will:

(1) Ensure that all weapons are serviceable and are maintained according to DA Pam 738-750 and TM 9- 1005-206-14p/1.

(2) Ensure the security of weapons and ammunition in accordance with in accordance with AR 190-11.

(3) Ensure that all personnel have qualified with their basic weapon in accordance with this regulation and, as a minimum, have fired for familiarization with any other authorized standard or nonstandard weapon prior to use.

(4) Report lost, damaged or unserviceable weapons to the supporting property book officer for report of survey and/or turn- in instructions. Lost weapons will be documented in accordance with AR 735-5 and must be reported through command channels with 24 hours.

(5) Submit equipment improvement recommendations through channels to Commander, USACIDC, ATTN: CISP-LO, in accordance with DA Pam 738-750.

(6) Ensure compliance with range safety rules as outlined in appendix R, AR 385-63, FM 23-9 and FM 23-35.

c. The supporting property book officer will report changes to the DoD Small Arms Serialization Program (DODSASP) and conduct the annual reconciliation validation in accordance with AR 710-2 and TM 38-214.

17-3
Authorization documentation

a. Special agents. In accordance with AR 190-14 and AR 195-2, the issuance of a DA Form 3638 (Criminal Investigator Credential) to Department of the Army special agents by the CG, USACIDC, authorizes the recipient to carry and use issued weapons. DA Form 2818 (Firearms Authorization) is not required.

b. Non-agent CID supervisors. The DA Form 2818 issued by a field grade CID commander superior to the individual receiving the form (in accordance with AR 190-14) will constitute authority for the carrying and use of issued weapons for operational investigative purposes.

c. Local national criminal investigators. When authorized to carry and use issued weapons for investigative purposes, a DA Form 2828 will be issued by the first field grade CID commander within the individual s chain of command.

d. CID support personnel. Normally CID support personnel are not issued or authorized to carry a weapon for operational investigative purposes. Should such a need exist, a request for such authorization will be submitted to the first field grade CID commander within the chain of command for approval and issuance of the DA Form 2818.

e. Attached personnel. Personnel attached to the CID field element to support the investigative mission must have a DA Form 2818 if the carrying and use of weapons is authorized. The DA Form 2818 must be issued by a field grade officer. If the immediate CID element commander is not a field grade officer, the supporting provost marshal providing the attached person to the CID element will issue the authorization, providing that the provost marshal is a field grade officer. If the immediate CID element commander and the supporting provost marshal are both not field grade officers, then the authorization is issued by the first field grade CID commander in the chain of command. If the authorization is issued by the provost marshal, the individual must still obtain concurrence of the CID element commander/supervisor and comply with CID instructions and the provisions of this chapter.

f. DA Form 2818. When used, this authorization may be granted for a period of time not to exceed one year, with inclusive dates specified on the form. A statement indicating whether the weapon is to be carried openly or authorized to be carried concealed will be placed on the reverse of the form. Renewal of the DA Form 2818 is dependent upon satisfactory firearms training and qualification. The immediate CID commander/supervisor may waive the requirement to physically carry the DA Form 2818 on the person for those individuals performing covert operations in which possession of such documents could compromise the mission or endanger the individual. Sufficient control must be maintained over

such operations to ensure authorization and personal identification can be verified if required.

17-4
Responsibility for establishing procedures for the carrying and use of weapons

The USACIDC unit commanders and supervisors will establish procedures to govern the carrying and use of weapons by authorized personnel under their command and control and to preclude the carrying and use of weapons by unauthorized personnel.

17-5
Authorized and prohibited weapons and ammunition

a. Privately-owned. The carrying or use of privately-owned weapons and ammunition while performing official duties is prohibited.

b. Basic. The basic issue weapon and ammunition will be carried and used for investigative operations unless the carrying and use of other weapons and ammunition have been authorized. Military police personnel assigned to combined undercover missions or operations under USACIDC direction and control may be authorized by the local USACIDC unit commander to carry and use basic weapon and ammunition provided they have qualified with the weapon. These personnel will also participate in scheduled range firing conducted by the USACIDC unit while they are under USACIDC control.

c. Other standard weapons. A USACIDC unit commander at all levels may authorize the temporary carrying and use of other standard government weapons and ammunition when required by operational necessity. This authorization will be documented in the case file. Note: This does not pertain to other standard weapons issued to and carried by attached personnel when a standard issue CID weapon is not available for their use.

d. Nonstandard

(1) Nonstandard weapons and ammunition are authorized in section IIIA (Supplement) of the Tables of Distribution and Allowances in accordance with CIDR 710-5.

(2) The USACIDC special agents and military police personnel assigned to undercover missions or operations under USACIDC direction and control may be authorized by local CID commanders to carry and use nonstandard weapons and ammunition. Nonstandard weapons and ammunition are not intended for routine

use; however, they may be issued when required to conceal the individual s law enforcement status or when additional weapon concealment is needed.

(3) Commanders will establish procedures to ensure that only authorized personnel will be issued nonstandard weapons and ammunition.

(4) After approval is granted and prior to issue, coordination with the supporting property book officer will be made to ensure accountability is established for nonstandard weapons and ammunition.

e. Ammunition. Special agents and authorized military police personnel will be issued 2 fully loaded magazines, 13 rounds each, for a semi-automatic pistol (operational ammunition), when they sign for the basic weapon. When issued a nonstandard weapon, two weapon loads of ammunition will be issued. See paragraph 17-17.

f. Familiarization firing. Other standard/nonstandard weapons and ammunition will only be issued to individuals who are qualified with the basic weapon and have completed a familiarization course for that other standard/nonstandard weapon within the previous twelve month period. The familiarization course will consist of the following segments as a minimum:

(1) Instruction on the operation of the weapon.

(2) Instruction on the safety features of the weapon.

(3) Firing a minimum of 25 rounds at silhouette or bull s eye targets at a range of 15 meters or less.

17-6
Policies governing the carrying of weapons

a. All CID special agents are issued a weapon on a permanent basis. The issued weapon will normally accompany the individual on all future reassignments for the duration of the individual's assignment within USACIDC as prescribed in CIDR 710-5. Unless specifically restricted from carrying a weapon or performing a specific mission where weapons are not required, the special agent will carry the issued weapon while performing investigative duties.

b. As a clarification to paragraph 2.2 (Authority to Carry Firearms), AR 190-14, the term "loaded" is further defined as a weapon with a cartridge in the chamber. Unless otherwise prohibited by this regulation, AR 190-14, or the local USACIDC Commander, when USACIDC personnel carry their assigned weapon on official investigative duty, the weapon will be carried loaded as defined in this paragraph.

c. Support personnel will not normally carry weapons.

d. Attached personnel carrying weapons issued by the parent organization, not the CID unit, must comply with issue/turn in instructions of the responsible officer issuing weapons. Such information and instructions should normally be included in a memorandum of understanding (MOU) which addresses the attachment and use of those personnel. Chapter 13 of this regulation describes the preparation and use of such a MOU for drug suppression personnel.

e. Personnel will not normally carry weapons when relieved from investigative duties pending action under the provisions of AR 195-3, when hospitalized, on leave, attending school, or when prohibited from carrying weapons by their supervisor or commander.

f. In accordance with AR 190-14, special agents and CID supervisors are authorized to carry weapons outside normal duty hours. This authorization will be supplemented by a memorandum signed by the unit commander and will include at least the following information:

(1) The name(s) of the authorized individual(s).

(2) A statement that, under the provisions of this regulation, the carrying of weapons during other than normal duty hours is authorized.

(3) Any specific restrictions on the carrying and security of weapons during other than normal duty hours.

g. Unless specifically restricted under the provision of paragraph 17-6e(3) above, the authorization granted in accordance with paragraph 17-6e extends to both on-post and off-post locations.

h. When local national criminal investigators carry weapons, they will comply with the provisions of this regulation, Status of Forces Agreements (SOFA), and host country laws and agreements.

i. Weapons in the possession of USACIDC personnel in civilian clothing will not be unnecessarily displayed.

j. Weapons will not be displayed while conducting interviews/interrogations.

k. It is the responsibility of the individual carrying a weapon to act in a manner that precludes adverse comments and not participate in events which reflect unfavorably upon the individual or the organization.

l. The consumption of alcoholic beverages while armed is prohibited unless required by operational necessity (e.g., surveillance inside a bar, undercover

operations during which it is necessary to maintain a cover or liaison visits when refusal might cause offense). In these situations, USACIDC personnel consuming alcoholic beverages in connection with their duties are responsible for their actions and are expected to exercise mature and responsible judgment and professional behavior. In any case, where there is advance knowledge that alcoholic beverages will be consumed and there is no valid requirement to have a weapon, the weapon will not be carried.

17-7
Policies governing the carrying of weapons on commercial aircraft

a. All USACIDC personnel whose official duties require them to carry a weapon while aboard any aircraft operated by a commercial air carrier will notify a responsible air carrier representative of the flight on which he intends to carry the weapon at least one hour before departure. Prior to boarding the aircraft, USACIDC personnel will identify themselves to a responsible representative of the air carrier and will present either travel orders annotated to reflect that the traveler is required to carry a weapon in conjunction with official duties or their credentials. When the mission would be compromised if the identity of the USACIDC personnel or the fact that they are carrying concealed weapons became known, the air carrier s representative will be requested to assist in limiting this information; however, the representative is required by Federal aviation regulations (FAR) to identify all persons carrying weapons to law enforcement and security personnel responsible for boarding security, the pilot in command and any other armed passengers.

b. If the individual s duties do not require access to the weapon between the time the weapon would be placed in checked baggage and return of the baggage after the arrival at its destination, the weapon will be unloaded and locked in the individual s checked baggage. The baggage must be hard-sided. A responsible representative of the air carrier will be notified the weapon is in the baggage and that it is not loaded. The weapon declaration tag provided by the air carrier representative must be placed inside the baggage containing the weapon. The individual will retain the key to the baggage. Where possible, ammunition will be stored in an item of baggage different from the item containing the unloaded weapon.

c. During flight, should an incident occur (e.g., interference with crew members), armed CID agents will not take independent law enforcement action unless assistance is requested by the captain of the aircraft.

17-8
Policies governing the use of weapons

In all cases, the use of non-lethal force such as physical hands on restraint will be the first priority for use. Deadly force will only be directed against persons in cases of extreme need when all lesser means have failed or cannot reasonably be used.

a. Normally, for USACIDC personnel, deadly force is only authorized for the following reasons:

(1) In self-defense, when in imminent danger of death or serious injury.

(2) To prevent serious offenses against a person or persons (e.g., murder, armed robbery, rape or violent destruction of property by arson or bombing).

(3) To apprehend a suspect believed to have committed an offense listed in (2) above.

(4) For other situations in which deadly force is authorized and additional guidance on the use of force, see AR 190-14.

b. The discharge of any firearm by a special agent, other personnel assigned/attached or detailed to a USACIDC element or MP personnel involved in combined operations with USACIDC will immediately be reported by the person firing the weapon or anyone else having knowledge of the incident to the individual's immediate CID supervisor. The CID supervisor will notify the CG, USACIDC, by the fastest available means through: (1) During duty hours - the office of the DCSOPS, HQUSACIDC, (2) After duty hours - HQUSACIDC Staff Duty Officer. This notification will not be delayed in order to obtain all of the facts and it should reach the CG, USACIDC, within four hours of the incident. Further notification will be made as significant facts develop.

c. When, upon review of a report of weapon discharge not involving death or personal injury, it is determined that insufficient information is available, the appropriate USACIDC major subordinate commander may initiate an inquiry to ascertain all available facts concerning the incident. A copy of the inquiry will be forwarded to Commander, USACIDC, ATTN: CIOP-ZA.

d. When the discharge of a firearm by a special agent, other personnel assigned, attached or detailed to a USACIDC element, or MP personnel involved in combined operations with USACIDC, whether or not in the performance of official duties, results in death or personal injury to any person, the appropriate major subordinate commander or the DCSOPS will appoint a disinterested special agent or CID supervisor to conduct an inquiry into the circumstances of the incident with particular attention given to whether the firing was within the use

of force guidelines in AR 190-14, this regulation, current case law and local SOFA/host nation agreements. This inquiry may be conducted and reported as a separate criminal investigation under the provisions of AR 195-2 and this regulation; as an inquiry utilizing the general guidelines of AR 15-6; or as an inquiry under the provisions of AR 195-3, as appropriate. A copy of the findings will be forwarded through the USACIDC major subordinate commander to the Commander, USACIDC, ATTN: CIOP-COP-CO.

(1) If the shooting results in the death of any person, the special agent(s) or attached MP/MPI, who were directly involved in the shooting will be suspended from active investigative duties, pending the results of the inquiry. During this period, the CID unit commander will take steps to assist the individual in dealing with post-shooting trauma through interface with medical support services and counseling.

(2) If the shooting results in only personal injury, the CID unit commander, at his discretion and based upon known facts and circumstances, will determine if the special agent or attached MP/MPI should be suspended pending the outcome of the inquiry. The unit commander should consider the use of medical support personnel and counselors to assist the individual through any post-shooting trauma or stress.

17-9
General

a. The USACIDC unit commander has direct responsibility for the security of weapons and ammunition which are not issued to an individual. General responsibilities are contained in
AR 190-11.

b. Individuals issued weapons and ammunition have personal responsibility for their security.

c. Issue and turn-in of weapons and ammunition will be accomplished in accordance with the provisions of CIDR 710- 5

17-10
Unit security

a. When weapons are not issued to authorized individuals, they will be stored in a unit arms room or Class 5 container according to AR 190-11, Chapter 2.

b. Standards for lighting, guard protection, surveillance, and key and lock control are provided in AR 190-11.

c. Ensure monthly sensitive items inventories are conducted and returned to the supporting property book officer in accordance with DA Pamphlet 710-2-1.

17-11
Individual security

a. Individuals who carry weapons will assure that the weapons are either under their immediate physical control, handled in accordance with paragraphs 17-7 and 17-11c of this regulation, or reasonably secured in their lodging.

b. Reasonable security at a lodging means that the weapon is secured in such a manner so that its presence is not readily apparent and it is not easily accessible to unauthorized persons. If feasible, the weapon should be secured in a locked container that is not easily removable from the premises.

c. When required by unusual circumstances, the individual may release the weapon and ammunition for safekeeping to a law enforcement agent or to the registrar or property custodian of a medical facility against written receipt providing the individual is reasonably assured that the firearm and ammunition will be adequately secured. If the individual is unable to retrieve the weapon and ammunition within a reasonable period, supervisors will arrange to have the property returned to USACIDC control.

d. Special agents will comply with weapon turn-in procedures in force at confinement facilities when entering same, unless the procedures do no appear to be adequate for safeguarding the weapon. Under no circumstance will a special agent or anyone under his/her control carry a weapon into a confinement facility without the knowledge and consent of the security force commander on duty.

e. All personnel assigned to a USACIDC element who are issued a handgun will also be issued a weapon safety lock. The lock will be issued as part of the special agent’s Organizational Clothing and Individual Equipment (OCIE). The lock will be placed on the weapon when stored within a residence, or secured in a location other than the arms room or in an approved container in lieu of an arms room. Accountability for the safety lock and accompanying keys is the responsibility of the individual. Purchase of replacement locks for the standard issued 9mm pistol should be coordinated through Technical Services Division at USACIL.

f. The requirements at paragraph e also apply to non-standard issued handguns. However, the USACIDC issued safety locks may not fit the various models of non-standard handguns. Commanders can use appropriate funding to

locally purchase safety locks for those non-standard handguns that cannot be fitted with the USACIDC issued safety locks.

g. Under only the most exceptional and unusual circumstances will CID investigative personnel temporarily store (not to exceed one hour) their assigned government weapon in a privately owned or government vehicle. Under these circumstances, the weapon will be stored in the locked glove box or trunk. Overnight storage in a vehicle is prohibited.

17-12
Loss, theft, unlawful disposition or recovery of firearms and ammunition

Whenever a USACIDC weapon or ammunition is lost, stolen, unlawfully disposed of, or recovered, the USACIDC unit commander will:

a. Report and document the incident as prescribed in AR 190-11, Chapters 2 and 8.

b. Immediately notify the supporting property book officer. The supporting property book officer will notify the DoD Weapons Central Registry in accordance with AR 710-3 and TM 38-214.

c. If warranted, initiate an investigation or inquiry of the incident. If an investigation or inquiry is conducted, a copy of the completed report will be forwarded to the Commander, USACIDC, ATTN: CIOP-COP-CO.

17-13
Authorization for use

a. Each special agent will be issued the standard M11 pistol and holster, IAW CIDR 710-5, for use while performing criminal investigation duties. The agent will turn in issued equipment to their unit supply upon their retirement, ETS, or permanent removal from investigative duties.

b. Agents who do not wish to use the standard USACIDC issue holster/purse may purchase their own holster/purse with personal funds. Any privately owned holster must provide essentially the same degree of concealment and security that the issue holster provides and be consistent with acceptable law enforcement practices. These holsters must:

(1) Have a safety strap or securely grip the weapon with elastic or spring pressure to preclude the weapon from falling out during physical activity.

(2) Be worn in such a manner that the holster and weapon are securely positioned to preclude loss.

(3) Make the weapon readily accessible to the wearer, while minimizing its accessibility to others.

(4) Be professional in appearance so as not to reflect unfavorably on the wearer or draw attention to the weapon if inadvertently exposed.

c. Agents should wear the same holster during range qualification and practice, whether issue or personally owned, that they normally wear for duty.

d. CIDR 710-5 authorizes the use of regular operating funds to purchase holsters for nonstandard weapons for use in support of covert operations. The supporting property book officer will be notified to establish accountability of such holsters as needed.

17-14
Exceptions to policy

a. Under normal circumstances while performing criminal investigative duties, only holsters specified in paragraph 17-13a or 17-13b will be worn.

b. Commanders and special agents-in-charge (SACs) may, on a temporary basis, authorize the wear of holsters which do not conform to paragraph 17-13b when operational requirements preclude wear of an authorized type of holster. Holsters authorized under these circumstances must comply with all of the following criteria:

(1) Provide optimum concealment.

(2) Minimize the possibility of injury to the wearer or to innocent parties.

(3) Minimize the possibility of losing the weapon.

c. If, due to operational necessity, the use of a holster is not practical or desirable, unit commanders will determine and approve the method by which the weapon is to be carried. In all cases, the handgun will be securely and safely positioned in a manner which will minimize the possibility of any unsafe condition such as dropping the weapon.

17-15
Loan of weapons and holsters

a. Subject to availability, USACIDC field unit commanders may hand receipt CID-owned 9mm pistols with accompanying holsters, to MP/MPI personnel assigned, attached, or detailed to a USACIDC element using the issue procedures in CIDR 710-5. The personnel must comply with the provisions of paragraph 17-11 and other instructions in this chapter as appropriate.

b. Prior to MP/MPI personnel using USACIDC weapons on any mission, their USACIDC supervisor will ensure that they qualify with the pistols in accordance with this regulation.

c. All USACIDC supervisors will ensure that MP/MPI personnel, who wish to carry their issue USACIDC weapons in privately-owned holsters fully comply with the provisions of paragraph 17-13b.

17-16
Oleoresin Capsicum (Pepper) Spray

a. General.

(1) Pepper spay is the third level in the use of force continuum. Its use is authorized in law enforcement situations only after verbal persuasion and other lesser means have failed.

(2) Use of pepper spray, when subduing an individual, is dangerous and can cause death if proper procedures are not followed. If a suspect is sprayed, intentionally or inadvertently, the individual will not be left alone. Special agents shall be alert to any indications that the individual needs immediate medical care. This includes, but not limited to, breathing difficulties, gagging, profuse sweating and loss of consciousness. Immediate medical assistance will be sought for individuals suffering such symptoms. When medical treatment is completed, medical clearance will be received before further processing the individual(s).

(3) Pepper spray will be reasonably secured when not carried. Cap-Stun OC pepper spray is biodegradable and does not require any special decontamination procedure. Disposal will be accomplished in accordance with local installation policy. Additionally, the item will be added to the monthly sensitive items inventory for accountability.

b. Responsibilities:

(1) Group commanders are responsible for budgeting/funding pepper spray requirements of subordinate elements. Additionally, group commanders are responsible for determining whether Status of Forces Agreements (SOFAs) and state laws in their areas of responsibility support issuance of pepper spray to special agents.

(2) Battalion/field office commanders will ensure the training requirements established by this policy memorandum are met as part of the Command Inspection Program. Additionally, battalion/field office commanders are responsible for procuring pepper spray based on recommended issue by subordinate offices. Coordination should be made with the Technical Support Division at USACIL for technical and purchasing advice prior to procurement.

(3) Detachment commanders/special agents in charge will determine which agents require pepper spray and must ensure that agents are properly trained in accordance with this guidance prior to issuing pepper spray. The training and authorization to carry pepper spray will be documented in the individual's training file. The determination to authorize pepper spray will be based on operational necessity, available funding and group/region approval for agents to carry pepper spray in their area of responsibility. Issuance of pepper spray is not mandatory.

c. Training:

(1) Special agents must have attended a certified training program prior to being issued an authorized pepper spray unit. A training manual applicable to two Cap-Stun models (Z 305 and Z 205) manufactured by ZARC International is provided at Figure 17-1. The Technical Support Division, USACIL, recommends these two models.

(2) Regardless of the type selected, similar training will be accomplished, using an appropriate inert training model, prior to issuance of the actual spray device. Per recommendation of the office of the Surgeon General (OTSG), pepper spray will not be sprayed on individuals during training to show its potential effects. The OTSG recommends using an inert training model for training purposes. Refresher training will be conducted annually.

17-17
Hollow-Point Ammunition

a. General

(1) This paragraph prescribes policy on the issue of hollow-point ammunition to CID special agents to carry in the United States and its territories.

(2) HQUSACIDC will procure the ammunition and ensure its delivery to Rock Island Arsenal. It is the responsibility of each major subordinate command (MSC) to arrange shipments from the Rock Island Arsenal to the designated Ammunition Supply Point. After the initial issue, each MSC must budget annually for hollow-point ammunition until it becomes available from the Army's inventory.

b. Restrictions

(1) Hollow-point ammunition will not be issued or carried in areas that prohibit its use based on Status of Forces Agreement (SOFA) or other laws. Supervisors will implement appropriate safeguards to ensure this does not inadvertently happen. Where its use is prohibited, ball ammunition will continue to be issued to special agents.

(2) Hollow-point ammunition will not be carried by agents in areas of armed conflict or military tactical theaters outside the United States and its territories.

c. Accountability and Issue

(1) Hollow-point ammunition will be accounted for and rotated in accordance with CIDR 710-5, Materiel Management System, paragraph 4.3, 3 May 96.

(2) As stated in paragraph 17-5, special agents will be issued 26 rounds of the ammunition when signing for the basic issue CID weapon, unless prohibited by SOFA or other laws.

(3) Where hollow-point ammunition is authorized for issue, commanders will maintain an additional 30% of their operational load as ball ammunition for issue to investigative personnel when traveling to areas that prohibit hollow-point ammunition. However, investigative personnel will not be issued both types of ammunition to carry at the same time.

d. Training

(1) Weapon qualification will continue to be accomplished using ball ammunition. Familiarization firing with hollow-point ammunition will be accomplished IAW Appendix P of this regulation.

17-18
General

Special agents, CID supervisors and civilian employees who are issued the M11 compact pistol must qualify with the weapon on the courses described in this regulation. The M11 pistol will not be issued until the individual has qualified in the use of the weapon and is familiar with the provisions of this chapter, AR 190-14, applicable SOFA/host nation agreements, and local law. All required M11 pistol qualification firings will be recorded on the CID Form 85-R (Practical Pistol Qualification Scoreboard). Special agents transferring to a new unit will carry this scorecard with them and turn it in upon in-processing at the gaining CID unit.

17-19
Weapons training

a. The M11 pistol is an individual weapon intended for use in close combat to save one's life and/or to prevent the commission of a serious crime. The M16 rifle is an individual weapon intended for use in combat in order to survive and win on the battlefield. All personnel must keep their assigned weapons in good working condition and have complete confidence in their individual marksmanship ability. This ability can only be attained through good study and thorough practical training.

b. The objective of practical training is to improve upon ones marksmanship skills, to demonstrate the capabilities and limitations of the weapon, and to familiarize the shooter in firing under conditions of stress. Proper training will develop the shooter s ability to fire quickly, instinctively and accurately.

c. Pre-marksmanship instruction (PMI) should be completed prior to qualification, pistol PMI is addressed in FM 23-35 and M16 PMI is addressed in FM 23-9.

17-20
Weapons qualification and sustainment

a. Practical weapons qualification is the measurement of the person's ability to obtain a minimum designated score on a firing course designed to simulate the actual conditions under which the weapon will ordinarily be used. Its purpose is to maintain the individual's skill and proficiency, reaffirm the weapons operation, and to confirm the individual aiming point and sight picture.

b. The nighttime M11 pistol sustainment course is conducted for the purpose of emphasizing the increased difficulty of successfully engaging a target in limited/complete darkness and that firing under such conditions increases the risk of danger and injury to bystanders. Because the lighting conditions influencing the nighttime firing scenario will vary considerably due to multiple conditions of which there is little control, the course will not be scored.

c. Shooters should be in good physical condition as the amount of proficiency will depend in part on the ability to assume prescribed positions quickly, instinctively coordinate body movements, and to complete the course within the prescribed time.

d. All personnel assigned or attached to CID units issued the basic weapon are required to conduct the following firing schedules and types of courses:

(1) All special agents, attached MP/DST members, supervisors, USACIL examiners, polygraphers and civilian investigators (to include procurement fraud investigators), not identified in paragraphs (2) and (4), who routinely carry their weapon or perform investigations, conduct technical investigative support in the field or perform PSU duties.

Frequency of Course: Quarterly for Practice Fire and Record Fire. Annually for Night Instructional, Night Practice and Night Sustainment.

(2) All special agents, CID agent supervisors, and polygraph examiners that are assigned to HQUSACIDC, USACIDC major subordinate commands, or other field unit staff positions.

Frequency of Course: Semi-annually for Practice Fire and Record Fire.

(3) All U.S. Army Reserve special agents and CID agent supervisors.

Frequency of Course: Annually for Practice Fire and Record Fire.

(4) All special agents assigned to USACIL-CONUS as examiners who do not perform investigations, conduct technical investigative support in the field or perform PSU duties.

Frequency of Course: Not required to qualify, but must qualify before carrying a weapon and assuming investigative duties.

e. Type S silhouette targets will be used when conducting M11 pistol firing. The CID Form 85-R will be used to record the daytime qualification scores and nighttime sustainment firings. The familiarization block is only for use with standard/ nonstandard weapons, other than the M11 pistol, as described in paragraph 17-5. The following scoring table will be used for daytime qualifications:

(1) Expert: 271-300

(2) Sharpshooter: 241-270

(3) Marksman: 211-240

(4) Unqualified: 0-210

f. Personnel who are issued nonstandard weapons in accordance with paragraph 17-5d of this chapter will fire the nonstandard weapons for familiarization prior to carrying the weapons for investigative activities. Familiarization firing will be conducted as prescribed by paragraph 17-5f, or in accordance with the most appropriate U.S. Army course. When a nonstandard

handgun is routinely carried, qualification firing and nighttime sustainment firing will be conducted as prescribed by appendix P and Q of this regulation. When a nonstandard weapon other than a handgun is routinely carried, qualification and night sustainment firing will be conducted according to the most appropriate U.S. Army qualification course.

g. The Protective Service Unit will establish a standard operating procedure (SOP) outlining procedures for issue, qualification standards, and firing course for nonstandard weapons used in support of that activity. Additional guidance for special agents assigned to the protective services unit is contained within DA PAM 350-38, for the H&K MP5 submachine gun and within FM 19-10 for the M1200 shotgun.

h. All personnel assigned M16 rifles are required to conduct M16 qualification annually. Qualification consists of the day record course, NBC, and the night record course. The NBC and night record courses are biennial events for U.S. Army Reserve personnel. Standards are contained in DA PAM 350-38.

17-21
Failure to qualify

a. If a special agent, CID supervisor, or civilian employee authorized to carry a firearm fails to meet minimum qualification standards for the M11 pistol, the following steps will be taken:

(1) The individual will be given the opportunity to re-qualify by firing the course again, that same day. The second firing will be done under the close supervision of a CID supervisor, who will monitor the individual closely to determine defects in the individual's shooting skills. Additional firings will be accomplished so long as ammunition is available and the CID supervisor feels the individual is demonstrating improvement and is likely to be able to meet minimum qualification standards.

(2) Should the individual still be unable to meet minimum qualification standards, the commander will withdraw authorization for the individual to carry a weapon in performance of duty and assign the individual to duty functions not requiring the carrying of a weapon. The CID supervisor will immediately schedule remedial firearms training and reschedule the qualification firing for that individual. The rescheduled qualification firing should be accomplished within 10 working days of the original qualification firing.

(3) Should the individual still be unable to meet minimum standards at the rescheduled qualification firing, the CID supervisor will continue a remedial firearms training program and give the individual all reasonable opportunities to successfully qualify during the next 30 days. If necessary, the individual should

be medically evaluated to determine if there is a medical cause contributing to the failure to qualify (i.e., vision problem, physical limitation, etc.). If the individual fails to qualify by the end of this 30 day period, the CID commander/special agent-in-charge will initiate action to have the individual s accreditation withdrawn.

(4) Should the individual be given a temporary medical profile limiting the individual's ability to carry or fire the M11 pistol, the CID commander will withdraw authorization for the individual to carry the weapon and limit duty assignments to tasks where the use/need for a weapon is not required. When the profile is no longer valid, the individual will be required to qualify with the pistol before being authorized to resume carrying the weapon in performance of duty. If the profile is made permanent and the individual is unable to carry/fire the weapon, or fails to qualify at the next scheduled firing, the CID commander/special agent-in-charge must initiate action for withdrawal of accreditation.

b. If an individual assigned the M16 rifle fails to meet the minimum qualification standards for the M16 rifle, the CID commander should initiate action per AR 601-280 or as deemed appropriate.

Figure 17-1: OLEORESIN CAPSICUM (PEPPER) SPRAY GUIDANCE

1. INTRODUCTION

a. This training guidance is applicable to all law enforcement personnel assigned to a USACIDC unit who carry CAP-STUN's Oleoresin Capsicum (OC) Spray (Pepper Spray). The manufacturer has authorized USACIDC to use its training program. This training program will not be disseminated for use outside USACIDC channels without the approval of ZARC International, INC. Any USACIDC elements electing to dispense pepper spray other than CAP-STUN's OC will develop their own training program applicable to the type of model selected for use.

b. Law enforcement has long recognized that a wide and dangerous gap exists in the range of tools available to them. The most common law enforcement tools, the nightstick and the gun, may be either too weak or too strong of a response to many situations. For years as an alternative to deadly force, law enforcement agencies have used chemical agents such as CN and CS that have proven to be unreliable and counterproductive.

c. In the early 1980s, ZARC offered the results of CAP-STUN's OC testing to the special agents in charge of the Less-Than-Lethal Weapon Study at the Firearms Training Unit of the FBI. During the summer of 1989, The Firearms Training Unit of the FBI Academy, Quantico, Virginia, completed three years of intensive research regarding CAP-STUN's chemical agent OC. As a result, the FBI authorized CAPSTUN for its agents and special weapons and tactics teams. It was through the efforts of the FBI that OC as a new breakthrough in chemical agents and less-than-lethal weapons was officially introduced in the form of a report to U.S. law enforcement in 1989.

d. This training guidance is provided for USACIDC personnel actively involved in law enforcement. This information provides individuals with pertinent information on OC spray weapons, its physiological effects, the appropriate circumstances and proper technique to use it and the procedures to be followed after use.

e. This guidance outlines principles, present techniques and skills in using CAP-STUN OC spray weapons to help control violent and aggressive behavior, and reduce personal injuries to personnel as well as subjects and the general public. Additionally, this guidance attempts to help reduce the civil liability exposure, which might normally be associated with trying to control violent, unruly, and aggressive individuals.

f. This guidance is for reference only. It is not designed to replace live training. Proper training and repeated practice are crucial factors for effective application.

g. The instruction in this guide should not be used for other brands of pepper or tear gas products, since the guide specifically pertains to the method by which CAP-STUN has been engineered and designed. Any USACIDC elements electing to use other brands of pepper will develop a training program applicable to the brand selected.

2. INSTRUCTIONS

a. All USACIDC special agents/investigators should be thoroughly trained in the safest possible use of OC spray weapons. Such training should include simulations of real life situation to refine skills.

b. All USACIDC training on OC spray weapons (CAP-STUN models Z-205, Z-305, and Z-606 will consist of:

(1) Identifying the psychological and physiological effects of OC spray weapons on subjects when sprayed.

(2) Identifying different OC spray weapon models and the capability of each.

(3) Demonstrating proper stances, and proper techniques in the use of OC spray weapons.

(4) Giving verbal commands and/or directions to non-compliant subjects in connection with the use of OC spray weapons.

(5) Procedures to be administered to subjects exposed to CAP-STUN.

(6) Methods of area decontamination.

c. The below listed warnings and cautions should be initially covered:

(1) OC spray weapons are severely inflammatory & irritating. The contents are flammable and are under pressure.

(2) Individuals armed with OC spray weapons should avoid accidental contact with eyes, skin or mucous membranes.

(3) Do not expose to heat, spark or flame or store above 120 degrees Fahrenheit (50 degrees Celsius). Do not puncture or incinerate can.

(4) Do not spray against the wind.

(5) Keep out of reach of children - not to be handled by minors.

(6) It is a crime to transport OC spray products on passenger aircraft.

3. TRAINING REQUIREMENT AND SUPPLIES

The recommended number of students for training per instructor should not exceed twenty-four (24). The instructor based on existing conditions and other factors may make class size adjustments. Requirements and supplies needed by the instructor and students are listed below:

a. What to bring to the class

(1) Pen and paper

(2) Casual clothing & athletic shoes

(3) Extra shirt

(4) Cloth face towel

(5) NO firearms or weapons

b. Instructor considerations

(1) Classroom area

(2) Outdoor open space for application

(3) Tables and chairs

(4) Training guidance

(5) Video camera and tapes (batteries or cords as needed)

(6) Towels (paper and cloth hand towels)

(7) Water supply/hose and buckets

(8) Mild liquid soap

4. WHAT IS CAP-STUN?

CAP-STUN is an inflammatory agent that swells mucus membranes causing immediate closing of the eyes, uncontrollable coughing, gagging and gasping for breath. CAP-STUN has clearly demonstrated its ability to instantly and consistently render aggressors incapable of resisting arrest or further violence for up to 45 minutes with no harmful after-effects. CAP-STUN has been successfully proven to be effective on subjects under the influence of alcohol and/or drugs,

emotionally disturbed subjects, or other subjects, who have reduced sensitivity to pain, as well as domestic and wild animals, without causing permanent damage. In addition, it causes a sensation of intense burning of the skin and mucous membranes inside the nose and mouth. Therefore, CAP-STUN appropriately applied to an assailant will cause a loss of coordination and upper body control, thus incapacitating and rendering the subject fully compliant. CAP-STUN has been used on a wide spectrum of subject profiles and in an extensive array of circumstances. CAP-STUN has been used worldwide by more than 2,000 law enforcement agencies such as Federal, State, County, and Municipal Police, State Highway Patrols, U.S. Prisons and Corrections Facilities, U.S. Military and Foreign Government Agencies.

5. WHAT DOES OC SPRAY DO FOR LAW ENFORCEMENT?

a. Provides a high probability of instantaneous control over highly aggressive, violent or emotionally disturbed subjects.

b. Effects those under the influence of narcotics or alcohol.

c. Supplies effective reaction to barricade situations.

d. Responds effectively to crowd control situations, where officers may want to disperse or subdue a mob.

e. Effectively restrains and controls single or multiple subjects.

f. Minimizes physical contact, reducing injury and other risks for both officers and subjects.

g. Effectively reduces or eliminates the need to escalate to a higher level of force in the use-of-force continuum.

h. Reduces incidents of law enforcement officers being shot with their own weapons.

6. PHYSIOLOGICAL EFFECTS

a. Proper applications of CAP-STUN OC spray will affect four major areas upon contact. The respiratory system, eyes, motor control and the skin (REMS). All effects are temporary, and will usually completely dissipate within 45 minutes. The CAP-STUN formula is an inflammatory agent that causes mucous membranes to swell.

b. REMS: CAP-STUN targets REMS rendering the subject incapable of resisting arrest and prevents aggressive behavior upon contact:

(1) Respiratory - causes uncontrollable coughing and gasping for breath.

(2) Eyes - forces the eyes to close immediately.

(3) Motor control - loss of body motor control, immobilizing an attacker immediately.

(4) Skin/mucous membranes - creates an intense burning sensation of the skin.

These physiological effects produce an instantly compliant subject who has lost coordination and upper body motor control, thereby precluding any further aggressive behavior.

c. Because of CAP-STUN's careful control of complex capsaicinoid levels, CAP-STUN can consistently produce REMS effect across the wide range of subject profiles including those under influence of drugs, alcohol, or mental disorders. All four REMS effects are necessary to render a subject incapable of resisting arrest or further aggressive behavior.

7. CAP-STUN'S INGREDIENTS ARE SAFE!

a. CAP-STUN has demonstrated no potential for long-term adverse health consequences in thousands of field uses. It contains the same alcohol (isopropyl/rubbing alcohol) present in perfumes and after-shaves. CAP-STUN has no long-lasting side effects or after-effects. In over 10 years of field experience, there has not been a single substantiated instance of adverse reaction to CAP-STUN by any subject with respiratory illnesses, heart problems, or poor reflexes. Spraying CAP-STUN directly at a subject will neither cause permanent eye damage (unlike stram spray pattern OC's) nor respiratory system damage, nor skin depigmentation.

b. In addition to its field use track record, CAP-STUN has undergone extensive toxicological testing in accordance with the procedures as outlined in U.S. Environmental Protection Agency (EPA) Health Effects Test Guidelines, EPA 560/6-82-001 and Pesticide Assessment Guidelines, EPA 540/9-82-025. These tests cover four key areas:

(1) Acute inhalation toxicity (LC50) test: To determine any toxicity level through the inhalation route of exposure. When tested, CAP-STUN's formulation was not found to be toxic to test animals when they were exposed to a concentration of 56.3mg/1, which is also the maximum and highest concentration that could be generated in the test system. Therefore the LC50 for CAP-STUN is far beyond 56,300 mg/m3 and no toxicity could be found at this maximum level.

(2) Primary skin irritation test: To determine the degree of skin irritation or damage. Beyond usual dermal irritation, CAP-STUN does not damage the skin.

(3) Guinea pig skin sensitization test: To determine any possibility of "allergy" with the test material. CAP-STUN is not a skin sensitizing or allergenic agent.

(4) Eye irritation test: To evaluate the potential of a test article to induce eye irritation or corrosion. Beyond short-term eye irritation, CAP-STUN does not cause eye damage.

8. FLAMMABILITY

a. There are some unfounded concerns about the alcohol content of CAP-STUN. CAP-STUN's formulation has been engineered specifically to perform safely and effectively and alcohol is currently the best available choice for the delivery of CAP-STUN formula.

b. Isopropyl alcohol within controlled environments does not cause any flammability problem. However, just as any other commercially available household aerosol, the spray should not be used at close range directly toward sparks or flames.

c. Isopropyl alcohol has a lower flammable limit (LFL) of 2.00 and upper flammable limit (UFL) of 12.7. In other words, it takes about 64 ounces of alcohol to reach the LFL level in 1000 cubic feet. (The LFL is the level of concentration in the atmosphere that is too minimal to burn). 64 ounces are approximately equal to 64 units of CAP-STUN standard duty model Z3-305 in a small room 10 x 10 x 10 feet - highly unlikely in an actual field situation. Just as one heeds warnings that come with equipment purchased for use at home or in the work place, one must heed warnings on the packaging of all weapons and, just like firearms safety, must be trained in the proper use of
CAP-STUN.

d. CAP-STUN has been carefully designed not to cause combustion under controlled and standard application. You may test this outdoors by spraying a lighted cigarette 5 feet from the nozzle away from any bystanders.

9. MATERIAL SAFETY DATA

Product safety information will be provided to those who provide emergency response medical assistance.

10. WHEN TO USE CAP-STUN

a. Because CAP-STUN causes no permanent injury, it may be introduced early in the use-of-force continuum. CAP-STUN normally falls between verbal commands and the necessity for physical engagement.

b. There are a number of force options available, but each individual agent must determine which option is most appropriate in a given situation, while taking into account other factors that might affect that particular set of circumstances and the use of force guidelines. Caution should always be emphasized for agents not to become too dependent on any single force option.

c. CAP-STUN use does not necessarily preclude the use of a greater level of force if necessary for officer safety or the safety and protection of others. CAP-STUN will not be used to replace the firearm, or any other equipment approved and issued by the USACIDC, but should be utilized as a force option within the use of force guidelines.

d. The use of OC spray weapons is to:

(1) Better defend yourself in the event of a physical attack.

(2) Aid and prevent injury to one-self or the subject when arrest is imminent.

(3) Protect citizens against harm, attack, or injury.

(4) To affect an arrest when violent or aggressive behavior is encountered.

(5) To prevent the injury of other persons or prevent damage to property subsequent to arrest.

(6) To control domestic or wild animals that are displaying hostile or aggressive behavior.

e. OC spray weapons should not be used against a person who:

(1) Submits peacefully to arrest and complies with lawful commands during an arrest.

(2) Complies with lawful commands during a valid investigative stop or while in-custody or detention.

(3) Is expressing mere verbal disagreement that does not threaten or incite others to threaten an officer and is not significantly delaying or obstructing discharge of duty.

Note: DoD, Army and USACIDC policy should be consulted for other inappropriate applications.

f. Do not use OC spray weapons against an attacker aiming a deadly weapon toward you. In these situation another alternative or a higher level of force may be justified. As with the use of any force option, use should rely heavily on agent experience and training, and should cease immediately when resistance or aggressive behavior ceases.

11. VERBAL COMMAND

a. If possible, verbal commands should always occur prior to the application of OC spray weapons. Verbalization achieves several things for the officer: First, it gets the officer breathing. Most untrained individuals hold their breath during a confrontation; thereby starving their muscles of much needed oxygen. When the human body is placed in a stressful situation, it reacts by going into what is called a "stress flood". In a matter of milliseconds, this stress flood causes various bodily responses to occur such as: rapid breathing, tunnel vision, adrenaline dump, and the excessive burning of oxygen converting glucose into short term muscle strength. When the officer shouts, "stop", "down", etc., this forces the air out of the lungs and over the vocal cords. The next response is to automatically fill the lungs by means of a deep breath, resulting in proper oxygenation of the lungs.

b. Verbal commands before, during, and after the confrontation must be practiced in order to use them under stress. Commands given before the actual use of OC spray weapons are essentially warnings that attempt to coax cooperation from the subject.

c. Prior to application: Give commands more applicable to the actual arrest procedure and not forewarn the subject about being sprayed, thus maintaining the element of surprise in the event of application.

d. After application: Again, commands directly applicable to the arrest; once restrained, agent initiates calming effects on subjects.

e. Position: Proper posture ensures effective use of CAP-STUN while maximizing agent safety. With your strong hand, hold the canister nozzle at the level of your ear, about 15 to 20 inches from your ear in front of your face, while the finger is on the trigger and the nozzle aimed at the subject's face. This posture will keep the canister away from the subject's reach and allow appropriate aim and distance from the subject. This is similar to the draw of an arrow in archery.

f. Stance: Approach or face the aggressor at a 45-degree angle. Your weak foot is forward and your strong foot is to the rear. Your feet should be shoulder width apart or wider. Your knees are slightly bent and the weight is equal on both feet. If an eminent encounter with an aggressor is anticipated, the CAP-STUN weapon

should be held in the strong hand along the strong leg (leg farthest from the aggressor) for immediate use.

g. Distance: For agent safety and maximum spray effectiveness, the agent should remain at a distance of 4 to 6 feet from the aggressor, depending on the situation. This is about normal interview distance and should allow the agent the much needed reaction gap in the event of aggressive action. If the unit is held within less than 4 feed range of the aggressor, the canister may be taken away with little or no chance of reacting.

h. Motions: If the subject is charging or running toward you while you are attempting to spray, the weak hand should remain open, palm facing toward the opponent and fingers pointing upward with no space between the fingers. There should be slight bend in the elbow. This posture helps prevent the aggressor from getting too close. Using a defensive push, the officer should disengage, move into a defensive position, allowing enough a gap between the subject and immediately spray. It is extremely important that immediately after spraying, the agent moves laterally, sidestepping the attacker, should the aggressor continue his body momentum forward.

i. Never step backwards while spraying; you should side step and exit laterally. In the event an aggressor using a weapon (other than gun) attacks an agent, the agent can exit the attack zone by lateral movement or may choose the use of CAP-STUN or other level of force depending on the situation.

j. Standard direct spray: This is the standard recommended method. The agent should aim the spray directly at the face of the subject between the eyebrows from a distance of 4 to 6 feet. A short one-second tap on trigger is required. If a subject fails to exhibit signs of submission and continues displaying aggressive behavior three seconds after being sprayed, a second short burst should be aimed at the mouth and nose.

k. Horizontal: With a slow twist of the wrist, while moving the spray horizontally from left shoulder to right shoulder, apply a sufficient amount of CAP-STUN while allowing for movement on the part of attacker. This method is used when the subject is moving around violently, and creates a mist of spray of 5 feet wide. When using this method the agent should rapidly move away from the mist, in order to avoid cross contamination of the agent.

l. Dry puff: By proper training, the user can achieve what is called the "dry-puff". The goal is to deliver a dry puff of the spray rather than wetting the subject with the liquid. Dry Puff rapidly delivers all capsaicinoids to the mucous membranes, producing immediate REMS effect. Dry Puff is achieved by:

(1) Duration: "Short" but adequate amount of spray. The longer the spray, the wetter the puff.

(2) Distance: The closer to the target, the wetter the subject. If you are too far, you may not deliver 100% of the load to the target.

(3) Since the manner in which an individual squeezes the trigger and the bodily agility of an individual during deployment varies from one to another, the user should find its best duration of spray and distance to produce a dry puff during training.

m. Saturation: This method is used when it is not possible to deliver CAP-STUN directly at the subject due to distance from the subject or artificial filtration fabricated by the subject. For example in a prison cell, the subject may have covered this/her face with a towel. Direct continuous spraying will provide partial REMS effect. It is therefore recommended that the "saturation" method be used. In this method CAP-STUN is delivered all around and above the head of the subject continuously in order to saturate the area with the airborne mist. Soon the mist will seep through the artificial filtration (towel) and will affect the respiratory system. Once the subject's face is exposed if necessary the direct spray at the face can be administered. Subject should then be moved immediately away from the contaminated atmosphere to eliminate difficulty in breathing.

n. Breath retention: Most individuals become highly defensive when they are sprayed with aerosol directly toward the face. The natural reaction is to close the eyes and hold the breath. Thus, ZARC recommends the following:

(1) Apply a true one-second burst toward the closed eyes. The capsaicin will immediately attack the mucous membranes of the eyes causing extreme burning sensation. The subject will have no choice but to automatically blink, causing CAP-STUN to enter directly into the eye lids which will immediately close the eyes.

(2) Immediately observe the subject. Due to extreme burning sensation of the eyes, it is a natural reaction for the individual to begin breathing. Immediately aim spray directly toward the chin and apply a one second burst on an upward swing of the wrist (move from chest to forehead) allowing the spray to enter into the nose and affect the respiratory system.

o. The following are common situations where agents must be prepared to deploy OC spray weapons properly:

(1) Ground: When an agent is down and the aggressor is up, the agent sprays the aggressor from the ground using the weak hand and feet to keep the aggressor from effectively continuing the attack.

(2) Multiple agents: In a situation involving more than one agent, the contact agent will shout "PEPPER SPRAY" and disengage. The agent verbalizing "PEPPER SPRAY", should spray the aggressor.

(3) Multiple attacker: In the event of multiple aggressors, the user should rapidly spray the aggressor who presents the most immediate threat and then others in order of threat or proximity.

(4) Indoor application: Spray directly toward the subject and quickly step away from the area while observing the subject closely. When subject is under control, remove all bystanders from the immediate area to avoid direct exposure to the mist. If any bystander is affected, calm them by assuring them that they will not be harmed and immediately begin post application. Ventilate the area by opening windows if possible. Do not use air conditioning for ventilation, since the OC spray mist could circulate to other unaffected areas. Caution should be used in certain environments such as nursing homes, hospitals, or any facility, which uses a central ventilation system. Do not use OC spray in hospital emergency rooms or other comparable areas.

(5) Barricade: The subject who barricades himself in an area, room, or building presents one of the most frequent and dangerous situations confronting the officer. The recommended application is as follows:

(a) Once the location of the subject is determined, the user should find a route to inject CAP-STUN into the immediate area of the subject with a TA (tubing attachment) model.

(b) Attach the tubing by squeezing the metal clamp onto the Z-505 nozzle. Remove needles cover and place the needle and tube into the cavity. If the subject is in the immediate vicinity, avoid inserting the needle too far to keep it away from the subject's reach. Make sure there are no tangles in the tube.

(c) Do not point the needle toward the ground but up toward the ceiling so that spray will come down like a shower. Pointing the needle downward will simply wet the floor with CAP-STUN. Do not bend the needle unless absolutely necessary for angled operation. The needle should be placed securely in the cavity since the pressure of spraying will throw the tube around.

(d) Hold can upright and begins spraying. It is usually recommended to empty the container, however depending on the interior space, you may want to use more or less.

(e) You should wait a minimum of 5 minutes before entering the space allowing time for the mist to travel to the designated area.

(f) Discard TA if clogged or if the needle has been bent. Do not attempt to clean the tube, since it should be replaced after each application.

(g) If officers are able to enter the building equipped with gas masks and several units of the Grenade (Z-606) model, they should place activated Z-606 upright in strategic positions in order to saturate the internal space around the subject with the airborne mist. It takes approximately 45 seconds for X-606 to empty. You should wait a minimum of 5 minutes before moving toward the location of the subject, allowing time for the mist to travel to the designated area.

(6) Large crowds: In this situation of civil unrest, there is a logical pattern to the crowd positioning and movement. Usually the crowd is on one side and the military police on another. Firearms and batons when used against rioters can result in casualties, mob retaliation, and unfavorable publicity. Many times the excessive use of force incites even greater violence. If CAP-STUN is to be used in an area that is inhabited, the residents should be notified in advance. This can be accomplished by personal contact or loud speakers notifying the inhabitants that CAP-STUN is going to be used and that all individuals should keep their doors and windows closed, turn off air conditioning units, and stay inside of the buildings or leave the area. The following is the standard recommended deployment in this situation, however USACIDC Agents and Military Police further refine their strategy skills through repeated practice.

(a) A line of military police soldiers equipped with Crowd Control model (Z-505) should begin spraying CAP-STUN toward the crowd from a maximum distance of 50 feet. The ratio is usually one officer to 10 individuals. Half of the officers should aim directly toward the chest level of the crowd and the other half should aim upward of 30 degree angle. This method produces a rolling mist of CAP-STUN that can travel well beyond 100 feet (depending on direction of air).

(b) It is important that the officers position themselves with the wind to their back. The wind will carry CAP-STUN into the desired area. Keep in mind that the air currents will vary due to buildings and other obstacles and that all of the units should not be used at the same time. Probably one Grenade model (Z-606) should be laid down in order to see the direction of the air currents.

(c) Several Grenades (Z-606) should be used to cover any avenues that are left open and need to be closed in order to redirect the crowd.

(d) If you are in a position where the individuals are upwind, it will be necessary to drop the Grenade (Z-606) approximately 25 yards behind them. This method of deployment will move the crowd in your direction along with CAP-STUN. It is necessary that the defense line immediately begins spraying Crowd Control (Z-505) toward the crowd the instant the crowd begins moving toward the defense line.

(e) It is absolutely necessary that a wide area with multiple units of CAP-STUN be covered in order for the subjects to receive a sufficient quantity of CAP-STUN so that they will not want to re-initiate their unruly activity.

(f) CAP-STUN can cause panic and fear. An avenue of escape should be left open for the subjects when cap-stun is deployed against unruly crowds.

(7) Animal control: One of the reasons CAP-STUN has achieved a high level of recognition is because of its ability to affect animals. Most animals are not affected by tear-gases, since they are not equipped with developed tear duct or lacrimatory glands. Although CAP-STUN's law enforcement and military aerosol product lines are not specifically designed to be used against attacking animals, in most instances CAP-STUN formula has proven to be effective against attacking dogs. The application of CAP-STUN is a safe and humane control approach without having to resort to a more serious course of action. The following factors should be considered, to deploy CAP-STUN against animals:

(a) The user should begin applying a three second burst the instant the dog charges from a distance in order for the dog to run into the mist. Animals are much faster than humans and can travel 30 feet within a fraction of time. If the spray is used when the animal has reached the user, it is too late.

(b) Once the dog has entered and passed through the mist and is within reach of the spray, a continuous two second burst aimed toward the nose (nostrils) should be deployed. Immediately allow extra distance to compensate for the animal's natural reflex to momentarily propel itself forward.

12. AFTER USE GUIDELINES AND REAPPLICATION

a. Upon delivery of final spray, the officer should allow approximately five seconds for the mist to dissipate and then verbalize specific and distinct commands. Do not rush into the mist cloud. Tell the subject exactly what you want him to do. In most cases, you should tell the subject to stand still and not move around.

b. One handed re-holstering after final application should be practiced. If an officer does not properly re-holster and drops the canister to the ground, friends of the person being arrested may spray him or her.

c. If circumstances allow, do not attempt to forcibly handcuff a sprayed subject immediately after spraying. Give the subject 30 to 60 seconds to react to the spray and overcome gagging or coughing. This gives the subject an opportunity to overcome the temporary effects of CAP-STUN on the respiratory system without the physical stress of handcuffing. Apply the proper procedure for approaching any potentially dangerous subject, and apply handcuffs or other

authorized restraining device(s) to complete the arrest. Secure legs to prevent kicking.

d. When CAP-STUN spray is inhaled, the respiratory tract is inflamed, and breathing is restricted. Hand-cuffing the subject behind the back while laying him/her on his/her stomach and placing pressure on the back or in any position that may cause difficulty in breathing such as maximal prone position may deny the subject proper breathing and cause positional asphyxia. Positional asphyxia occurs when body position interferes with respiration.

e. Subjects should be closely monitored and reassured that they are safe and will be cared for. They should be told to try to breathe normally and relax as much as possible. Instruct the subject not to rub the eyes. Normal breathing should resume within 5 minutes. If not, medical attention should be sought.

f. Under normal circumstances, all other symptoms should disappear within 30-45 minutes. If symptoms persist beyond 45 minutes, seek medical attention immediately. Make sure material safety data is available for the medical attendant.

g. All subjects should be asked if they are suffering any serious medical condition. Look for a Medic Alert bracelet or necklace on the subject. Ask the subject if he/she suffers from any respiratory diseases or problems such as asthma, bronchitis, and emphysema. If yes, seek immediate medical attention.

h. Subjects sprayed with CAP-STUN should be removed to an area of fresh air (uncontaminated air) and faced into the wind.

i. Do not leave an individual who has been sprayed with CAP-STUN unattended until the effects are completely diminished and the subject indicates he/she has fully recovered from the effects of the spray.

13. SPECIAL ATTENTION SUBJECTS

a. The following subjects are in "special attention" category for medical emergencies:

(1) Subjects substantially impaired by alcohol or drugs.

(2) Subjects who are breathing very rapidly, or sweating heavily, or exhibiting pale, ashen or colorless skin.

(3) Very obese subjects with a known medical condition like diabetes, a seizure disorder, asthma, emphysema, or heart trouble, and/or are of advanced age.

b. For subjects with bad heart conditions, the emotional stress of arrest may provoke a heart attack. Subjects with severe asthma can suffer a fatal bronchial attack from emotional or physical stress, even though force used to arrest was minimal. Although it is the stress of arrest and not the use of CAP-STUN that places certain categories of subjects under the special attention group, try to monitor a "special attention" subject at all times during and after arrest until the subject is released from custody or turned over to another agency.

c. Special attention subjects should be hand-cuffed with hands in front, not behind the back, unless agent safety considerations make that too dangerous. Transport the subject in an upright position with a seat belt buckled. Do not transport subjects lying face down or face up on the back seat. Do not "hog tie" subject by connecting foot and hand restraints. Do not gag subject or cover the mouth or nose.

d. Monitor the level of consciousness and breathing of the subject. While uninterrupted monitoring is not possible, officer should attempt to look at and talk to the subject on a frequent basis during custody. Subject should not be left alone in a car or in a room for any period of time. Do not assume a silent prisoner is asleep or harmlessly intoxicated.

e. The agent should seek immediate medical attention if the subject demonstrates the following symptoms:

(1) Loses consciousness.

(2) Stops breathing.

(3) Suddenly becomes incoherent.

(4) Begins to hyperventilate.

(5) Starts to look very sick.

14. TRANSPORTATION

a. If practical before transporting, cool water may be used to flush subject's face and eyes. However, this should not be attempted at the risk of the agent's safety.

b. During transportation, carefully monitor the subject's activity and watch for signs or breathing difficulty, unconsciousness, nausea, etc.

c. Ask the subject if he/she wears contact lenses. If yes, assist the subject in removing them from the eyes. Subjects wearing contact lenses should remove them, if possible, before flushing the eyes with water during the decontamination

process. Contaminated glass or hard lens can be later cleaned with soap and water, however any soft lens must be discarded.

d. If possible, use cool water to flush the face and eyes. Flush the eyes and tell the subject to separate the eyelids with his/her fingers. Tell the subject NOT to RUB the eyes. Absolutely no commercial eye wash should be used during decontamination process. Flushing should relieve eye inflammation within 15 minutes.

e. Cleaning affected skin areas with a non-oil base soap or liquid soap and water will expedite recovery by removing the resin from the skin. Once this is done, pat dry with a cloth towel. A wet towel or ice packs may be used on the affected areas to reduce inflammation.

f. When the subject is turned over to a facility, the arresting agent should ensure that the custodians of the facility are informed of the fact that the subject has recently been sprayed with CAP-STUN.

g. If the subject's hair has been sprayed, subject may experience a burning sensation of the face when he/she is taking a shower.

h. If clothing has been soaked and wet with CAP-STUN's orange mist, simply wash the clothing with detergent as you usually launder the clothing.

i. The agent should avoid touching his/her eyes, nose, mouth and other sensitive skin areas until he/she is able to wash their hands.

j. Warning: There are decontamination sprays available on the market to be used for tear-gas and OC. ZARC cautions against the use of such sprays decontamination chemicals against CAP-STUN. Agencies should avoid using any other chemicals for decontamination of CAP-STUN.

15. AREA DECONTAMINATION

CAP-STUN's formulation is not a particulate. It is biodegradable and does not require any special decontamination procedure. Normal ventilation will remove the CAP-STUN spray from the environment within 45 minutes. This is a breakthrough in the chemical agent decontamination process as it eliminates the necessity of contracting with professional firms specializing in decontamination procedures. Savings in insurance can also be obtained since most insurance companies are aware of the serious and costly decontamination problems involving CN and CS tear gas agents.

Figure 17-1: OLEORESIN CAPSICUM (PEPPER) SPRAY GUIDANCE

CHAPTER 18

18-1
Purpose

This chapter establishes policy and procedures for the USACIDC Criminal Intelligence Program.

18-2
Scope

This chapter provides guidance, responsibilities, and procedures concerning:

a. The types of intelligence data to be collected.

b. The collection, analysis, retention, and dissemination of criminal intelligence.

c. The reports and forms to be used for data gathering and reporting.

d. The management and administration of the program.

18-3
Objectives

This program furthers the USACIDC investigative mission by providing:

a. A standard means of recording, processing and disseminating criminal intelligence.

b. Policies and guidance to safeguard intelligence data from unauthorized disclosure.

c. A systematic approach to criminal intelligence which:

(1) Facilitates the control of criminal activity.

(2) Identifies crime conducive conditions.

(3) Provides investigative leads.

(4) Identifies crime patterns and trends.

18-4
Policy

It is USACIDC policy that all CID elements will maintain an active criminal intelligence program to support their investigative operations.

a. Required reporting will be accomplished in accordance with this chapter, AR 25-50, Preparing and Managing Correspondence, and AR 25-55, The Department of Army Freedom of Information Act Program.

b. Automated and manual files required by this program will be maintained and disposed of in accordance with AR 25-400-2, The Modern Army Record keeping System (MARKS) or AR 380-5, Information Security Program, and CIDR 25-1, Microcomputers, Microcomputer Policies, Procedures and Standards.

c. Release of criminal intelligence will be accomplished in accordance with the guidance in AR 340-21, The Army Privacy Program, and Chapter 25 of this regulation.

d. All investigative personnel will actively participate in the criminal intelligence process.

18-5
Policy exception

Requests for exceptions to the provisions of this chapter will be submitted with justification to HQUSACIDC, ATTN: CIOP-COP-PO

18-6
Responsibilities

a. The office of the Deputy Chief of Staff for Operations (DCSOPS) (CIOP-ZA), HQUSACIDC will:

(1) Develop policies, guidance, and regulatory changes as required.

(2) Define and identify training requirements.

(3) Coordinate with appropriate Federal and DoD/DA staff agencies on policy issues affecting the criminal intelligence program.

(4) Periodically evaluate program effectiveness and recommend improvements.

b. The Intelligence Division (CIOP-IN), HQUSACIDC will:

(1) Conduct selected studies of criminal intelligence issues.

(2) Coordinate intelligence activities with DoD/DA staff elements, major Army commands, and other law enforcement agencies.

(3) Initiate Criminal Alert Notices and Bulletins.

(4) Disseminate Criminal Intelligence Reports (CIR), CID Form 97, as appropriate.

(5) Review and evaluate all CIRs, forwarded to HQUSACIDC to identify modus operandi, crime trends, and other systematic problem areas.

(6) Maintain a centralized HQUSACIDC system capable of maintaining, recording, and retrieving selected items of information provided by the CIR reporting process.

(7) Prepare CID HQ Form 476, Index to Criminal Information Report work sheet, from CIR information and forward to CRC, Data Processing Division.

(8) Evaluate existing criminal intelligence indices for continued retention. Purge as appropriate and advise CRC of purged records.

(9) Review and disseminate information from the Dun & Bradstreet and Consolidated Individual Contracting Action Reports upon request from field elements.

(10) Develop and disseminate command-wide Essential Elements of Criminal Intelligence (EECI).

(11) Identify and periodically disseminate a command- wide CID Information Digest of current criminal modus operandi.

(12) Serve as alternate point of contact and processor of all Financial Crimes Enforcement Network (FINCEN) requests.

(13) Maintain the Violent Criminal Apprehension Program (VICAP) database.

c. The Director, Crime Records Center (CICR-ZA), HQUSACIDC will:

(1) Data reduce those criminal intelligence data collection sheets obtained from the Intelligence Division.

(2) Disseminate to the Intelligence Division quarterly indices and coordinate with the Intelligence Division concerning the retention/purging of the files.

(3) Incorporate name check searches of indices as a part of the name cheek process in support of on-going criminal investigations and military police investigations.

d. Each USACIDC major subordinate commands will:

(1) Manage the criminal intelligence program within their AOR.

(2) Designate a criminal intelligence manager within their AOR.

(3) Ensure that subordinate district/field offices, as appropriate, have individuals assigned to perform duties as a criminal intelligence manager within their respective AOR.

(4) Coordinate criminal intelligence matters, as necessary, with appropriate military, Federal, state, and foreign law enforcement agencies.

(5) Develop EECI efforts. Copies of USACIDC major subordinate command EECIs will be provided to HQUSACIDC, ATTN: CIOP-IN.

(6) Review criminal intelligence reports submitted from subordinate elements and, when appropriate, further disseminate data outside their AOR.

(7) Identify and request training requirements to the office of the DCSOPS, HQUSACIDC.

(8) Conduct periodic reviews of the program in their AOR.

(9) Develop and maintain an intelligence collection plan for their AOR.

e. All USACIDC district/field offices commanders will:

(1) Implement the provisions of this chapter within their AORs in accordance with policies and guidance prescribed by HQUSACIDC and the appropriate USACIDC major subordinate command.

(2) Designate a criminal intelligence manager within their AOR.

(3) Designate a criminal intelligence manager at subordinate offices within the AOR when appropriate.

(4) Ensure that the CIRs are in compliance with this chapter. This will not preclude timely release of a CIR by a subordinate unit.

(5) Ensure that subordinate elements initiate explicit requirements for the review of EECIs by all special agents assigned.

(6) Ensure that subordinate elements participate in the criminal intelligence program. The responsibility for administrative functions will be determined by the parent organization.

f. The criminal intelligence manager will:

(1) Act as the focal point for all criminal intelligence within his AOR.

(2) Process CIRs and maintain and dispose of the files required by this chapter.

(3) Plan for, process, coordinate, collate, analyze and reevaluate all data relating to criminal intelligence.

(4) Orient new personnel in the criminal intelligence operations.

(5) Ensure that CIRs are generated on available criminal intelligence and that the CIRs are appropriately disseminated in accordance with this chapter.

(6) Disseminate developed or received criminal intelligence to other law enforcement agencies or supported activities, as appropriate, in accordance with AR 195-2. This may be done verbally and by memorandum.

(7) Ensure that EECI administration includes, at a minimum, a sequential numbering system, title, and termination dates. All responses to a EECI will refer to the EECI number and title.

g. Special agents will:

(1) Coordinate with the criminal intelligence manager during the initial stages of any preliminary inquiry, investigation and/or crime prevention survey (CPS) to identify data relevant to the investigation.

(2) Furnish data developed during any preliminary inquiry, investigation and/or CPS to the criminal intelligence manager for analysis and retention.

18-7
General

This chapter provides guidance on the intelligence processing system and collection planning.

18-8
Intelligence processing

a. Information is developed from various sources (refer to appendix S for types of sources of information). Referrals and allegations of criminality come from military personnel and units, other police agencies, and the private sector. Investigators develop information as a routine course of duty. As stated in paragraph 9a, AR 380-13, "No information will be acquired about a person or organization solely because of lawful advocacy of measures in opposition to U.S. Government policy, or because of activity in support of racial and civil rights interests. Paragraph 9, AR 380-13, contains other restrictions on types of information that may be collected. Personnel involved in collection of criminal intelligence should familiarize themselves with AR 380-13.

b. The criminal intelligence manager must analyze and evaluate all of the information. The information processed by the criminal intelligence manager generally falls into four categories: raw data, significant data, local interest information , and command interest information.

(1) Raw data. This is the least substantive of the four basic categories of information. Many items of information are too fragmentary to justify initiating investigative activity or reporting. When collected and carefully analyzed, some items of data, which individually are apparently insignificant, can often be assembled to form meaningful information and significantly contribute to the effectiveness of the overall criminal intelligence program. The fact that this type of information is often fragmentary makes it important that the information be properly analyzed and additional collection efforts made, as needed, to corroborate the information.

(a) Raw data folders will be controlled by administrative file number, title, and year groupings. Sequence numbers will be assigned to each raw data folder. Raw data files may be categorized, if necessary, to facilitate information filing and retrieval and may be initiated on a monthly, quarterly, semiannual, or annual basis depending on the volume of information flow into the office. The purpose of breaking down the folders into less than an annual folder is to allow for easier administrative handling, research, and retrieval of information.

(b) A raw data file will consist of a CID Form 28, Agent Activity Summary, and/or a copy of the DA Form 2804, Criminal Data Reference Card, or computer generated report used in place of the DA Form 2804, which reflects unsubstantiated, fragmentary information received at a USACIDC office. The raw data files will be continuously reviewed to determine if matching information exists which would upgrade the information to significant data or necessitate other investigative actions/reporting.

(c) To preclude undue administrative burden, the raw data file will not be annotated to indicate "No raw data received on this date" or other similar expressions.

(2) Significant Data/Target Analysis. The criminal intelligence manager, as appropriate, will coordinate all investigative activity/analysis to be performed on the significant data/target analysis folder with the appropriate special a gent, operations officer and/or special agent-in-charge. Many items of information are substantive enough to justify immediately initiating a significant data or target analysis folder. Other times, an analysis of the DA Form 2804, or automated data report will reveal corroboration or the development of more substantive information. When sufficient information concerning previous intelligence and/or individual(s) is received or developed to merit upgrading raw data to significant data, a separate sequence number action will be initiated. Anytime raw data is upgraded to significant data or a ROI is initiated, the cross reference index card DA Form 2804, or automated data retrieval system will be annotated to reflect the sequence number assigned. To further ensure retrievability, if raw data files are used in addition to the DA Form 2804, or automated data system, the actual documents containing the raw data should be annotated with the sequence/ROI number.

(3) Local interest information. Information considered by the operations officer and/or special agent-in-charge to have interest and application only to the immediate area need not be disseminated above that level. The majority of information developed will be of this category. However, this should not be construed as precluding the transfer of intelligence information about a suspect from one investigative location to another so that the receiving office may follow up, as appropriate. Information transferred from one investigative unit to another should be disseminated to the appropriate USACIDC major subordinate command and to HQUSACIDC, ATTN: CIOP-IN.

(4) Command interest information. Information considered by the operations officer and/or special agent-in-charge to have interest and application at HQUSACIDC levels will be reported in a Criminal Intelligence Report.

(5) The fact that Tommy Tent-Pegs is caught using and distributing dangerous drugs within his unit would be of local interest. The fact that he may be stealing Government property on his own and at adjoining posts and installations ma y be of broader interest. The fact that he is transporting the drugs across country or state lines may be of USACIDC major subordinate command or USACIDC command-wide interest. The fact that he is using a military logistical system, i.e., supply, air craft, mail, would be of command wide interest.

c. The criminal intelligence manager then collates the data according to its importance and its interest to the local element, higher headquarters, and other agencies. Collation results in an intelligence profile and identifies requirements f

or dissemination to those with a need for the data. Other information of potential value is retained for further evaluation.

d. A crime analysis guide is provided at appendix T.

18-9
Collection planning

a. When sufficient raw data has been collected to indicate the need for establishment of a significant data folder, a collection plan should be developed by the special agent subject to review, coordination and concurrences of the agent's supervisor and criminal intelligence manager. This plan should identify potential criminal intelligence, provide for the targeting of collection efforts on significant data, and identify law enforcement or other agencies from which information should be requested.

b. As the collection plan is executed, previously collected data is evaluated in light of newly developed information. From this, an intelligence profile identifying areas of interest should emerge. These areas will include crime patterns, methods of operation, individual suspects, and locations.

18-10
General

This chapter identifies the general categories of information to be collected, analyzed, and reported, implements program collection and processing phases, and provides guidance on records and files management.

18-11
Records management

a. Intelligence information files will be maintained by the criminal intelligence manager separate from other investigative files in the office. The criminal intelligence manager will control access to the files. A cross reference or dummy folder will be placed in the main investigative/administrative files to reflect that criminal intelligence files are maintained by the criminal intelligence manager.

b. The following files, at a minimum, will be maintained where a criminal intelligence manager has been appointed. In order to facilitate program management, coordination, and analysis of crime patterns and trends, similar files should be maintained at the USACIDC major subordinate command level.

(1) The DA Form 2804, Crime Records Data Reference - This is a multi-copy form designed to be used as an input document to the intelligence process. The form can be used to input data into a manual retrieval system and serve as a cross reference/index card. For automated systems, see section IV of this chapter.

(a) The DA Form 2804, or automated data record will be completed each time a suspected criminal event transpires for which no report of investigation is prepared, on receipt of source information, or when the criminal intelligence manager determines that data retrieval may be required for later analysis. A separate form should be used for each incident/event. The form will be prepared by the person receiving the information. The criminal intelligence manager may assist, a s needed, in preparing the form. If additional information is needed by the criminal intelligence manager, use the remarks section and/or back of the form.

(b) Instructions for filling out this form are reflected in AR 195-2. The form provides one original document and one copy. When three additional copies of the form are made, investigative searches can be conducted through a logical and straight forward sequence.

(c) Within the index and cross reference file, a minimum of four sub-files will be created and a copy of the DA Form 2804 filed in each. The original copy will be placed in a sub-file titled "NAME", the first copy will be placed in a sub-file titled "MO", the second copy will be placed in a sub-file titled "OFFENSE", and the third copy will be placed in a sub-file titled "LOCATION". The fourth copy may be placed in a target/collection, raw data, or source folder. The fifth copy will be retained at the originating office. At the USACIDC major subordinate command and district/field office level, the fifth copy may be used at the discretion of the unit commander/operations officer.

(d) The copy of the form placed into the offense file will be separated by the major offense code. To preclude the creation of numerous sub-files for offense codes, it is suggested that the offense code sub-file not be broken down further than the first two to three digits of the offense code. It is not necessary that sub-files be created for every offense code but rather for those primary offense codes that are most frequently used. In the offense code for property, it may be necessary that a subset be created to identify property as either being stolen or recovered.

(e) When a form is placed into the offense file, a check of that file should be conducted to determine if there is any matching data.

(f) A DA Form 2804, or automated data record will be prepared on intelligence reports received from other USACIDC elements/investigative agencies if the report is to be retained.

(2) Raw data. These folders are controlled by sequence numbers and title (i.e., drug, economic crime, etc.) DA Form 2804, or automated data record will be completed on information in these files.

(3) Significant data/target analysis. Active working files controlled by sequence numbers will be retained by the special agent to whom the file is assigned. The criminal intelligence manager should maintain a separate folder to track active working files to show the general subject matter of the file and where it is assigned (individual or team). Closed files will be maintained by the criminal intelligence manager. If a prior DA Form 2804, or automated data record exists on the information in the significant data folder, the form will be annotated to reflect the existence of the file.

(4) Criminal Alert Notices (CAN). These will be filed in sequential order by year group. DA Form 2804, or automated data record will be completed on all criminal alert notices that are retained.

(5) Criminal Intelligence Reports (CIR)

(a) Those generated by an office will be filed in sequential order by year group. Since these reports are sometimes related to targeted activity, separate folders may be created with copies of those reports which apply to a specific functional area, i.e., one folder might contain a listing of reports on each register manipulations, another might contain a listing of reports on merchandise receiving problems.

(b) CIRs received from other offices will be evaluated for retention only, or further action. If a CIR is for retention only, an annotation will be made in the raw data folder and a DA Form 2804, or automated data record will be prepared if necessary. The incoming CIR will be retained in a raw data folder. If an office has more than one raw data folder, the incoming CIR will be placed in the folder which is specific to the subject.

(6) Criminal Intelligence Bulletins (CIB). These will be filed in sequential order by year group. Since these bulletins sometimes relate to targeted activity, separate folders may be created to list those which apply to a specific functional area, i.e., one folder might contain a listing of reports on merchandise receiving problems. A DA Form 2804, or automated data record will be completed on those that are retained.

(7) If there is matching or like information, the form(s) should be pulled and reviewed by the criminal intelligence manager in coordination with the operations officer special agent-in-charge to determine what action should be taken.

18-12
Information collection

The following types of criminal activity are some areas (although not all inclusive) which can be targeted for specific information collection efforts:

a. Diversion, theft, and/or manipulation of Army supplies, equipment, or logistical procedures/systems.

b. Bribery, fraud or fraudulent practices in appropriated or nonappropriated fund activities.

c. Organized groups committing crimes on U.S. Army installations.

d. Thefts of Army weapons/munitions.

e. Narcotics/dangerous drugs.

f. Violent/disruptive activities on or directed at Army installations.

18-13
Sources of information

The sources of information available are limited only by the imagination and initiative of those engaged in an intelligence collection effort. The following sources of information are accessible through HQUSACIDC and re quire specific information for access:

a. Dun & Bradstreet. This is a reporting service on more than seven million U.S. and international companies and corporations. The Business Information Report (BIR) generated by Dun & Bradstreet includes information about a company/corporation worth, associates and officers, subsidiaries, company operations and history along with information from public records, i.e., public filings and legal actions. Dun and Bradstreet also produces a Government Activity Report (GAR) on companies doing business with DoD and non-DoD agencies. The GAR listing is beneficial when contract information is needed on contracts with a small monetary obligation. Unlike the GAR, a DD-350 contract listing is available on firms at no cost to this headquarters. This listing provides information on contracts with obligated funds more than $25,000 for DoD and non-DoD contracts. This listing is compiled from DD Form 350s submitted by individual purchasing offices for contracts from the current fiscal year plus 3 fiscal years before. See the Dun & Bradstreet/DD-350 User Handbook.

(1) Dun & Bradstreet/Government Activity Reports. Requests for Dun & Bradstreet/Government Activity Reports will be submitted to the Intelligence

Division utilizing a Financial Crimes Enforcement Network Research Worksheet (figure 18-5) in accordance with paragraph 18-13d

(2) It is important to remember that this information is intended for lead purposes only and may not constitute a factual picture of a company's position in the business community.

b. Obtaining information from the U.S. Customs Service on monetary transactions under the Bank Secrecy Act.

(1) The U.S. Customs Service is the central repository for reports filed pursuant to the Financial Record Keeping and Currency and Foreign Transactions Reporting Act of 1970. They maintain a data base that contains IRS Form 4789, Currency Transaction Report, Customs Form 4790, Report of International Transportation of Currency or Monetary Instrument Report, and Treasury Form 90-22.1, Foreign Bank Account Report.

(2) Requests for Bank Secrecy Act data should be made in writing from the head of the local office to the local U.S. Customs special agent-in-charge. Requests may be standard letter format, but must include the specific names to be checked, any identifying data available, what violations of law are being investigated, and a summary of the investigation.

(3) Requests for name checks by foreign offices of the DoD should be forwarded to the local U.S. Customs attaché.

(4) Requests for evidence required for the court presentation must be made in writing by the Commander, HQUSACIDC, to the following address: U.S. Customs Service, Chief, Currency Programs Section, 1301 Constitution Avenue, NW, Washington, DC 20229.

c. The El Paso Intelligence Center (EPIC), Drug Enforcement Administration (DEA), U.S. Department of Justice. This center has the responsibility to provide a comprehensive and accurate intelligence picture of drug movement by land, sea, and air throughout the world as it relates to the United States; provide tactical support through the exchange of time sensitive information dealing with drug movement; and support other programs of interest to EPICs participating agencies, such as alien smuggling and weapons trafficking.

(1) Requests for information from EPIC will be submitted only by the USACIDC-EPIC Liaison Officer (LNO), USACIDC major subordinate command drug coordinators or others at USACIDC major subordinate commands and higher levels who have be en authorized to access EPIC.

(2) Information from EPIC will normally be obtained by an electrical message transmitted to EPIC through the USACIDC-EPIC LNO via the following

addressee line: LNO, USACIDC-EPIC LNO Ft Bliss, TX //CIRFB-LNO//. Such messages will be marked with the caveat "FOR OFFICIAL USE ONLY." Authorized personnel in CONUS may contact EPIC at 1-800-351- 6047/48 only when an immediate response is needed that involves a pending arrest or possible dangerous situation to investigative personnel. An information copy of all requests sent to EPIC will be provided to HQUSACIDC, ATTN: CIOP-CO. EPIC will not routinely search their data bases on information they receive for input. All requests for EPIC responses must fully identify the requesting individual (name, location, SSAN, telephone number, and organization) and USACIDC as the originating agency.

(3) Significant intelligence concerning drug trafficking/smuggling developed from raw significant data files will be provided to EPIC by the USACIDC major subordinate command drug coordinator or others using an electrical message if it has not been otherwise provided in a serious/sensitive incident report.

d. FINCEN.

(1) This network is a multi-source financial intelligence, analysis and targeting network designed to generate new leads relative to the financial aspects of criminal activity. It is a joint Federal law enforcement operation utilizing the intelligence databases of the Internal Revenue Service, Drug Enforcement Administration, U.S. Customs, U.S. Postal Inspection Service, Federal Bureau of Investigation, U.S. Secret Service, Bureau of Alcohol, Tobacco and Firearms, and others. A wide variety of databases can be accessed, to include Narcotics and Dangerous Drugs Information Service (NADDIS), U.S. Postal Inspection Service (ISDBIS), INTERPOL Case Tracking System (ICTS), Financial Database (FDB), credit bureaus and business reports to include Dun & Bradstreet reports.

(2) Send requests directly to the USACIDC liaison at FINCEN for Authorizing Official signature and analysis. FINCEN requests may be sent via facsimile at (703) 905-3526 with a cover sheet, or e-mail the electronic form to ChrisR@fincen.treas.gov. If your office needs a copy of the current FINCEN Request Form (TDF 90-22.44 (Rev 03/01), or has any questions regarding FINCEN please contact CID SA Rebecca Christensen at (703) 905-3541.

18-14
Essential elements of criminal intelligence (EECI)

a. The EECI will be used to direct information collection efforts at specific criminal activity within USACIDC's area of investigative responsibility. The EECI will be prepared so that the recipient is able to focus upon specific items of inquiry during a collection time frame. EECIs will be issued either by HQUSACIDC, or a USACIDC major subordinate command.

(1) Command-wide EECI. Issued exclusively by the Intelligence Division. Each USACIDC major subordinate command is encouraged to submit recommendations for a command-wide EECI to the office of the DCSOPS, HQUSACIDC.

(2) Each USACIDC major subordinate command will ensure that each EECI published by their headquarters is limited in application to their area of responsibility. A Copy of the USACIDC major subordinate command EECI and consolidated results, when compiled and analyzed, will be forwarded to HQUSACIDC, ATTN: CIOP-IN, so that they may be evaluated for command-wide dissemination.

b. All EECIs will be disseminated by either message or memorandum. Telephonic transmission is authorized in cases of emergency however, such action must be followed up by written copy as soon as possible. A sample format for a EECI is at figure 18-1. All EECI transmissions will:

(1) Display a sequential control number consisting of the year and number of EECI for that year. Example: 01-1, 01-2, etc.

(2) List, in order of priority or sequence of events, specific queries to be addressed by the recipient during collection efforts.

(3) Provide a rationale for each query to inform operational elements of background information to aid them in focusing their collection effort.

(4) Provide a specific date by which the recipient will report collected information to the initiator. At least one reporting date will be established during the active life of the EECI.

(5) Provide a specific date that the EECI will be terminated. EECI will not remain in effect for longer than one year.

(6) The last paragraph of each EECI will list previous EECIs published from the headquarters which are still in effect. This will assist field elements to account for those EECIs for which they are responsible.

c. All EECI recipients will:

(1) Use a sequence number action to commence collection efforts and develop information.

(2) Report all information developed on the EECI to the initiator in a CIR format. Each query in the EECI will be addressed, even if a negative response is provided. Recipients can reply on CID Form 97 or by message format. When

there is a complete negative response to the EECI, reply by electrical message or electronic mail.

d. USACIDC major subordinate commanders will:

(1) Establish uniform policies for the filing and disposition of EECIs at USACIDC major subordinate commands and subordinate elements according to AR 25-400-2.

(2) Ensure that the USACIDC major subordinate command and subordinate elements initiate requirements for the collection effort in response to EECI queries. Include correlation to relevant ROIs, CPSs, CIRs, and other investigative actions. In addition, coordination should be effected with local law enforcement agencies, both military and civilian, to solicit any information they might possess which pertains to the announced EECI.

e. The Intelligence Division, HQUSACIDC will:

(1) Collect, maintain, analyze, and publish all relative information that is reported from the field.

(2) Coordinate intelligence gathered between field units on related information.

(3) Advise USACIDC major subordinate commanders on the collection efforts in their AOR.

18-15
Intelligence reporting

a. The Criminal Alert Notice (CAN). The purpose of a CAN is to expedite the reporting of perishable information to organizations external to CID. A CAN will be used for the dissemination of crime related, time sensitive information such as serial crime, fraud schemes, bad checks and impersonators. One reason for the use of a CAN is to attack the offender's capability of victimizing others and to alert high-risk activities (such as exchanges, banks and hospitals) in an event to prevent them from being victimized by a given suspect. In order to reduce duplicate reporting, incidents, topics or matters reported in a CAN will not be reported in CIR. CID Elements will assign appropriate case file numbers (ROI/Sequence) to CANs. A CAN may be initiated from an existing investigation, or the can may be initiated as a separate case. Distribution of CANs will be limited to the area of responsibility of the CID element originating the CAN. Superior CID elements in the chain of command may reissue the original CAN within their respective areas of responsibility. Only HQUSACIDC is authorized to issue worldwide CANs or to post CANs to national level law enforcement bulletin boards (such as LEO). A copy of the Can will be provided via electronic mail

(whenever possible) to the originating CID element's parent field office/district/battalion, group and to HQ,USACIDC at ciopin@belvoir.army.mil. See figure 18-2 for instructions and format for preparing a CAN.

(1) CAN Sources. Information concerning criminal activities may be received from various sources, including, but not limited to:

(a) Army and Air Force Exchange Service (AAFES)

(b) Open Mess Activities

(c) Finance Offices, Credit Unions and banks

(d) Commissaries

(e) Other Law Enforcement / Investigative Agencies to include Military Police, AFOSI, NCIS and DCIS.

(f) CID Investigative Files and Sources

(2) Criteria for CANs. As a general rule, CANs will be published only on incidents or matters that CID investigates.

(3) Recommendations for a worldwide CAN will be submitted via electronic mail to HQUSACIDC at ciopin@belvoir.army.mil.

(4) Responsibilities.

(a) Any CID element publishing a CAN must ensure that the appropriate installation(s) chain of command (to include the SJA and PAO) and local investigative agencies (e.g., military police, FBI, AFOSI, NCIS, civilian police as appropriate) in their geographical area are briefed on the matter being reported. Coordination with the supporting SJA and PAO is critical for any CAN that is to be released to the public or posted in a public place.

(b) If additional information (i.e., apprehension, use of a different name, etc.) is developed, either a supplemental CAN will be issued (under the same case file number) or the CAN will be withdrawn from circulation, as appropriate.

b. Criminal Intelligence Report (CIR) preparation:

(1) A separate sequence number action will be initiated to prepare a CIR, even if the information comes from an ROI or other on-going investigative effort.

(2) The special agent who develops the information normally will prepare the report and have it reviewed by the criminal intelligence manager. It will be in a

narrative format as set forth in figure 18-3. Minimum quotas for CIRs will not be established. Quality reporting of intelligence data is the desired goal.

(3) The report may be quite brief (a summary of activities) or complex (a collection of documents/diagrams/photographs). The report should be tailored to the needs of the principal recipient, be objectively presented so that the recipient can act on the basis of accurate intelligence, and be structured so that the findings are described logically and concisely. The report must separate positive information from hypothesis and inference, and contain only information that USACIDC is authorized to collect and retain.

(4) If the report mentions a suspect, full identification, when available, will be included in the report so that proper indexing and later retrieval may be accomplished. The report will normally identify individuals, companies, or other entities suspected of being involved in criminal activity. An individual "name only" listings, without a date of birth or other piece of unique identifying data (i.e. SSAN), must be avoided.

(5) Unless the report contains classified information, it will be marked "For Official Use Only."

(a) Normally, reports will be transmitted via regular mail although an electrical message or electronic mail may be used. Reports considered to be sensitive/classified will be forwarded via appropriate secure means.

(b) HQUSACIDC, ATTN: CIOP-IN, will be provided a copy of any reports provided to agencies outside the military investigative community.

(c) Information from reports may be provided to other law enforcement investigative agencies in a letter of transmittal with a caveat that the report may not be made a permanent part of any records filing system or further disseminated outside their agency. HQUSACIDC, ATTN: CIOP-IN, will be provided a copy of all such reports.

(6) Additional CIRs will be submitted upon the development of any additional or new information, i.e., the initiation of an investigation based on the information contained in the original report, any new information developed which exonerates those initially listed in the report, or any new information which indicates the information contained in the original report was erroneous. The additional report will be distributed to every agency that received the original report.

(7) Information requiring immediate reporting, as a result of its significance or criticality, may be forwarded by electrical message or electronic mail. A written report is not required after submission of a report by electrical mess age or electronic mail.

(8) A CIR will be used to report the following:

(a) Significant crime patterns.

(b) New methods of operation.

(c) Information relating to organized crime.

(d) Modern technology used by criminals.

(e) Substances and tactics used to negate Army drug testing procedures.

(f) Any intelligence concerning terrorists, terrorist groups or terrorist activities. (This information should be shared with the local Military Intelligence elements, as well as being forwarded to HQUSACIDC, ATTN: CIOP-IN.)

(g) Other information as reflected in paragraph 7-32a, of this regulation (i.e., investigative delays, lack of photographs when they would have added to the understanding of or help verify/depict evidence of an offense, polygraph declinations and examination results, etc.).

The above listing is not meant to limit the submission of CIRs however, it is meant to ensure the CIR remains a valuable internal source of information

(9) The offense code 9H, as a minimum, will be listed as the last offense code at the end of each CIR Report number. Other offense codes applicable to the CIR will precede the 9H offense code.

(10) CIR distribution.

(a) CIRs will, as a minimum, be sent to the supporting USACIDC major subordinate command and HQUSACIDC, ATTN: CIOP-IN.

(b) Supporting districts, field offices or resident agencies may require themselves to be placed on distribution of a CIR prepared by their subordinate elements.

(c) CIR may be sent laterally from the preparing office to another office which is identified as having a need for the information in the CIR.

18-16
Criminal Intelligence Bulletin (CIB)

These are based upon criminal intelligence reports, reports of investigation, crime prevention surveys, and other information acquired by HQUSACIDC and

the USACIDC major subordinate commands. Criminal intelligence bulletins are forwarded to all field elements to alert them of conditions, techniques, or situations which could be a significant factor in present or future investigations or crime prevention surveys. This information generally has application directly or indirectly throughout the command or a particular USACIDC major subordinate command. The dissemination of information in this specialized manner, rather than by a letter or message, is due to its importance and potential impact upon USACIDC operations or those of counterpart military and civilian law enforcement agencies. Criminal intelligence bulletins require special handling to ensure the information they contain is thoroughly disseminated to all who have a need-to-know. See figure 18-4 for format of the report.

a. Command-wide CIBs are prepared by HQUSACIDC. Suggested topics for command-wide CIBs from USACIDC major subordinate commands and field elements are encouraged and will be submitted to HQUSACIDC, ATTN: CIOP-IN.

b. Each USACIDC major subordinate command may prepare CIBs for their area of responsibility. Copies will be provided to HQUSACIDC, ATTN: CIOP-IN.

c. Each criminal intelligence bulletin will be assigned a sequential control number to assure accountability. This will be placed on the criminal intelligence bulletin following the office symbol. Example, CIB 94-1.

d. Upon receipt, criminal intelligence bulletins will be reviewed by operations officers, criminal intelligence managers, and special agents-in-charge to determine the applicability of the information to local operations. Name, offense, location and modus operandi information may be cross checked, to determine if related information is on file at the receiving unit which needs to be considered in local operational matters. Information available to the receiving unit that would serve to amplify, clarify or confirm what is contained in the criminal intelligence bulletin, should be provided to the office originating the bulletin.

e. All USACIDC unit commanders and special agents-in-charge will establish procedures to ensure each special agent reviews each criminal intelligence bulletin received.

f. Each USACIDC major subordinate command and district/field offices are authorized to make appropriate distribution of criminal intelligence bulletins provided such distribution will not jeopardize their ongoing investigative activities.

18-17
General

This chapter provides initial guidance on the implementation of the automated collection and processing aspects of the criminal intelligence program. The automated system will be structured to provide quicker response to inquiries needed by investigative personnel concerning ongoing investigations. Data input for the automated system may come from a DA Form 2804, sequence actions or review of open or closed report of investigation. An automated/computerized system may be used in place of the DA Form 2804

18-18
Automation implementation

a. Raw Data, significant data, or other source information developed at the local level will be entered into the criminal intelligence program.

b. In the event that an automated system is utilized, the DA Form 2804 is not required. Information from raw data files, etc., can be directly entered in the computer without the DA Form 2804.

c. If a disk/tape weekly backup is not maintained on computer data and stored for system recovery, a hard copy printout (backup) from the system or a DA Form 2804 file will be maintained

18-19
System description

a. The foundation for automation is to provide a standard and systematic cross-referencing scheme identifying installation criminal activity by major subject area.

b. The data input form can be a DA Form 2804 or similar document/form. This input form will be completed at such time as a criminal event transpires, on receipt of source information, or when the criminal intelligence manager determines that data retrieval may be required for later analysis.

c. When automated resources are available, instruction materials will be provided for use of the equipment to facilitate automation of the process described in this chapter.

Figure 18-1. Sample of Essential Elements of Criminal Intelligence (EECI)

FROM: CDR USACIDC WASH DC //CIOP-IN//
TO: AIG 9012
UNCLAS
SUBJECT: HQUSACIDC EECI 94-2, FORGERY AND LARCENY

A. CIDR 195-1, CHAPTER 18.

1. RECENT INFORMATION SUGGESTS PERSON(S) UNKNOWN ARE SENDING FORGED LETTERS TO BANKS IN CONUS WHICH DIRECT ELECTRONIC FUND TRANSFERS FROM A VICTIM'S ACCOUNT TO BANKS IN ASIA. THE NAVY HAS AN ACTIVE CASE WITH THIS MO, INVOLVING MULTIPLE VICTIMS, ONE OF WHOM IS A GENERAL OFFICER. THUS FAR EACH FORGERY HAS INSTRUCTED THAT A PERCENTAGE OF THE ACCOUNT BALANCE, NOT A SPECIFIC DOLLAR AMOUNT, BE SENT VIA "TELEGRAPHIC TRANSFER." ADDITIONALLY, ALL VICTIMS ARE EITHER ASSIGNED OVERSEAS, OR HAVE RECENTLY TRAVELED IN ASIA. THIS EECI IS FORWARDED IN ORDER TO DETERMINE THE MAGNITUDE OF THE PROBLEM, IDENTIFY SUSPECTS AND DEVELOP PATTERNS.

2. COLLECTION ELEMENTS:

A. ROI OR SEQUENCE NUMBER CONTAINING REPORTED INFORMATION.

B . NAME OF VICTIM'S BANK.

C. TYPE OF ACCOUNT, SAVINGS, CHECKING, OR MONEY MARKET.

D. BANK TO WHICH FUNDS WERE TO BE SENT.

E. ACCOUNT NUMBER AND NAME OF HOLDER.

F. WHAT PERCENTAGE OF THE ACCOUNT WAS REQUESTED?

G. HOW MUCH MONEY WAS TRANSFERRED AND WHEN?

H. ARE COPIES OF DOCUMENTS DIRECTING TRANSFER AVAILABLE? IF SO, PROVIDE COPY, IF NOT, WAS IT A LETTER, TELEX, ETC.

I. WHERE DID THIS DOCUMENT OR TELEX ORIGINATE?

J. DOES THE VICTIM KNOW HOW HE AND HIS BANK ACCOUNT WERE TARGETED, I.E., MONEY TRANSACTIONS IN FOREIGN COUNTRIES, LOST OR STOLEN CHECKS, ETC.

K. IDENTIFY ANY SUSPECTS DEVELOPED, OTHER THAN THE NAME OF THE RECIPIENT ACCOUNT HOLDER NAMED IN PARAGRAPH E ABOVE.

L. CITY AND COUNTRY OR RESIDENCE OR ASSIGNMENT OF VICTIM AT TIME OF INCIDENT.

3. COLLECTION OF THE ABOVE ELEMENTS IS NOT INTENDED TO CAUSE ADDITIONAL INVESTIGATIVE ACTIVITY. THE INFORMATION SHOULD COME FROM USACIDC FILES, OPENED AS OF 1 JAN 93. EACH LETTER/INCIDENT SHOULD BE REPORTED SEPARATELY IN THE ABOVE FORMAT.

4. RECIPIENTS OF THIS EECI WILL RESPOND IMMEDIATELY TO QUERIES AS INFORMATION IS GATHERED THROUGHOUT THE "LIFE" OF THE EECI. AN INITIAL RESPONSE THAT ADDRESSES INCIDENTS REPORTED AS OF RECEIPT OF THE EECI WILL BE FORWARDED NLT 15 JAN 94. NEGATIVE REPLIES, OR REPLIES WHERE NO DOCUMENTATION DESCRIBED ABOVE IS AVAILABLE, SHOULD BE MADE BY ELECTRICAL MESSAGE OR ELECTRONIC MAIL.

5. THIS EECI IS EFFECTIVE ON RECEIPT, AND WILL BE CANCELLED ON 15 APR 94.

6. TO ENSURE EECI FILES ARE COMPLETE, ADDRESSES ARE REMINDED THAT ONE OTHER HQUSACIDC EECI, 94-1, REMAINS IN EFFECT.

7. CID REPORTS ARE EXEMPT FROM AUTOMATIC TERMINATION OF PROTECTIVE MARKING IN ACCORDANCE WITH CHAPTER 3, AR 25-55.

Figure 18-1. Sample of Essential Elements of Criminal Intelligence (EECI)

Figure 18-2a. Criminal Alert Notice (CAN) Instructions and Sample

Criminal Alert Notices

1. Processing recommendations for worldwide CANs: USACIDC major subordinate command recommendations for worldwide CANs will be submitted, via electrical message or electronic mail to HQUSACIDC,
ATTN: CIOP-IN in the following format:

a. The "subject" portion of the message should reflect "Criminal Alert Notice," identifying the crime (e.g., murder, etc.), and any individual identification information.

b. Paragraph 1 will reference the source and reliability of the information.

c. Paragraph 2 will contain entities involved.

d. Paragraph 3 will contain known aliases.

e. Paragraph 4 will contain known social security numbers.

f. Paragraph 5 will contain a summary of all pertinent information developed to date on the suspect.

g. Paragraph 6 will identify the actions which the recommending unit wishes to be taken by the activities and agencies to be briefed. This would include such things as "detain suspect and notify Military Police/USACIDC," etc.

h. Paragraph 7 will contain a point of contact, including name and DSN number, from the recommending unit.

i. Paragraph 8 will contain comments for USACIDC units. For example, "This message is intended for direct release to all activities/agencies identified to be briefed. Suggest entire message be reproduced and military police assistance solicited."

2. Refer to the next page of this figure for a sample of the report.

Figure 18-2a. Criminal Alert Notice (CAN) Instructions and Sample

Figure 18-2b. Criminal Alert Notice (CAN) Instructions and Sample (Continued)

From: CDR USACIDC WASH DC //CIOP-IN//

To: AIG XXXX

(Classification)

Subject: CRIMINAL ALERT NOTICE (CAN) 01-XX: MURDER AND DESERTION

A. CIR 1234-01-CID000 and SEQ 1234-01CID000-12345

1. SUBJECT: DOE, John Quincy; SGT; 123-45-6789; 1 Jan 66; male; other; 60 inches tall; 150 lbs; black hair; green eyes; no known scars or physical marks.

2. On 5 May 94, DOE became involved in a verbal altercation, which escalated into a physical altercation. DOE shot SGT Joe Friday, resulting in his death. DOE fled the area. His current whereabouts are unknown.

3. It is suspected DOE is armed with a 12 gauge shotgun and should be considered dangerous.

4. This information is provided to alert other law enforcement elements of the possibility of DOE in their area of operation.

5. If you have any information on the above individual or have any questions contact SA Gilbert or SA Sullivan, Fort Swampy Resident Agency, DSN 123-4567 or commercial (123) 456-7890. Photos of DOE are available upon request.

6. The POC at this headquarters is CPT Danger, DSN 999-9999 or (999) 999-9999.

Figure 18-2b. Criminal Alert Notice (CAN) Instructions and Sample - Continued

Figure 18-3a. Criminal Intelligence Report (CIR) Instructions and Format

Criminal Intelligence Report Instructions

1. Criminal Intelligence Report Format. The following information will be included in the specified format for submission of any Criminal Intelligence Report, whether through electronic mail or CID Form 97. An example of an electronic mail Criminal Intelligence Report and a CID Form 97 is located at the next pages of this figure. If the report requires additional pages, use consecutively numbered pages. Attach as enclosures any other documentation, if needed.

Item 1. The heading shall be "Criminal Intelligence Report."

Item 2. Date Prepared. The date entered will be the date that the Criminal Intelligence Report is written, not the date of the information.

Item 3. Preparing Office. Self explanatory.

Item 4. Sequence Number. Commence this block with the notation "1st CIR," then list the assigned sequence number. Each subsequent CIR on the same subject matter will be numbered consecutively, e.g., 2d CIR, 3d CIR, and etc., utilizing the same sequence number. The sequence number will be followed by the offense code(s) that most appropriately describes the activity reported. The offense code 9H will not be used by itself.

Item 5. Title. Enter as much of the following information as possible: last name, first name, middle name, rank, social security number, year of birth, sex, race, alias, and unit or home address. Entries such as none, unknown, or ETA should be avoided, whenever possible.

Item 6. Offense/Type of Information. List the offense, if applicable, as defined in the UCMJ or Federal Criminal Code.

Item 7. Date Received. Leave blank, for recipient use.

Item 8. Case Number. Leave blank, for recipient use only.

Item 9. Synopsis.

a. Any reference related CIR or ROI numbers will be indicated in the first paragraph.

b. Source of Information. A short comment will be made in the second paragraph on the source of the criminal intelligence being reported and on the agent's evaluation of the reliability of the information, where applicable.

c. Narrative. The narrative will contain a brief, simple narrative in sufficient detail to enable a reader unfamiliar with the matter to understand what has transpired without reference to other documents or records. If the CIR is considered a completed action, the closing statement will be "This is a terminal report." If the CIR contains all available information but there is a possibility that additional information will be developed, the closing statement will be "This is a terminal report, no further reports are contemplated pending receipt of additional criminal intelligence." If the action will obviously require additional reports, the closing statement in the CIR will be "Additional Criminal Intelligence Reports will be submitted as information is developed."

Item 10. Signature Blocks. The CIR will possess both the signature block of the agent preparing the CIR and of their criminal intelligence manager or special agent-in-charge.

Item 11. Warning Statement. Every CIR will possess the following warning statement: "This document is intended for law enforcement personnel, intelligence analysts, military personnel and other officials with a need to know. Further dissemination of this report should be limited to a minimum, consistent with the purpose for which the record has been furnished, i.e., effective enforcement of civil and criminal law. Additional release requires prior approval from the CG, USACIDC, ATTN: CICR-ZA, Fort Belvoir, VA 22060."

Item 12. Distribution. At a minimum the following copies of the CIR will be sent and annotated in the block: one copy to HQUSACIDC (ATTN: CIOP-IN), one to the USACIDC major subordinate command, one copy to each office or outside law enforcement agency that the information pertains to, and one copy kept on file. HQUSACIDC will not disseminate CIRs for the originating office.

Figure 18-3a. Criminal Intelligence Report (CIR) Instructions and Format

Figure 18-3b. Criminal Intelligence Report (CIR) Instructions and Format - Continued

CRIMINAL INTELLIGENCE REPORT
(Formless Format)

Date Prepared: 22 Jun 99

Preparing Office: 1st MP Det, 3rd MP Group, Fort Example, FL 33141-5000

Sequence Number: 1st CIR - 0030-01-CID001-7F9G3/9H

Title: DOE, John Quincy; SGT; 123-45-6789; 1966; Male; Other; Alias "J.D."; A Company, 71st Ordnance Battalion, Fort Example, FL 33141

Offense/Type of Information: Larceny of Government Vehicle (tactical wheeled)

Date Received:

Case Number:

Synopsis:

a. Reference: ROI 99-CID001-12345

b. Source of Information: This information was provided by the Fort Swampy Provost Marshal and is considered reliable.

c. On 5 May 99, at 0200 hours, a Military Police patrol observed an individual, later identified as SGT DOE, entered the unsecured l/5th Transportation Battalion motor pool and droving off in a M1028 High Mobility Vehicle (HUMMV), serial number 010-010-1001. Previously, CPT DANGER, SGT DOE's Company Commander, had overheard SGT DOE inquiring as to the potential resale value of HUMMVs. On 11 May 99, SGT DOE was apprehended by Officer Dudley, Atlanta Police Department (NFI) at an Atlanta, Georgia used car dealership (NFI) while trying to sell the stolen HUMMV. This is a terminal report.

///ORIGINAL SIGNED///
Ann D. Gilbert
SA, 4321

///ORIGINAL SIGNED///
John W. Smith
SA, 1234
Criminal Intelligence Manager

DISTRIBUTION: This document is intended for law enforcement personnel, intelligence analysts, military personnel and other officials with a need to know. Further dissemination of this report should be limited to a minimum, consistent with the purpose for which the record has been furnished, i.e., effective enforcement of civil and criminal law. Additional release requires prior approval from the CG, USACIDC, ATTN: CICR-ZA, Fort Belvoir, VA 22060.

1 - HQUSACIDC, Fort Belvoir, VA, ATTN: CIOP-IN; 1 - HQ, 3rd MP Group, USACIDC; 1 - File

Figure 18-3b. Criminal Intelligence Report (CIR) Instructions and Format - Continued

CHAPTER 19

19-1
Purpose

This chapter prescribes policy and procedures for managing the acceptance and accreditation of USACIDC personnel IAW AR 195-3 (Standards for Acceptance, Accreditation, and Release of United States Army Criminal Investigation Command Investigative Personnel).

19-2
Applicability

This policy applies to all Active and Reserve Component USACIDC field elements.

19-3
Application Process for Military Investigators

a. Prospective applicants initiate the process by contacting the nearest CID office.

b. Initial Interview Process:

(1) The special agent-in-charge (SAC) or their designated representative, or reserve component equivalent will conduct an initial interview to determine whether the potential applicant is qualified to apply for acceptance into the special agent program as specified in this chapter and AR 195-3.

(a) If a determination is made that an applicant lacks the law enforcement requirement, then the procedures for internship (Chapter 20) will be accomplished. An application received from a soldier participating in the intern program will be processed in the same manner as a fully qualified applicant.

(b) The representative will review the Realities of the Investigative Profession (Figure 19-1) with the perspective applicant and have the applicant sign the document.

(c) Prospective applicants cannot possess any of the disqualifiers specified in AR 195-3.

(d) Prospective applicants who meet or surpass the standards provided in AR 195-3 may apply for acceptance into the special agent program.

(2) CID application checklist is provided at Figure 19-2.

(3) The SAC or their designated representative, will obtain a signed disclosure release statement (Figure 19-3). The Privacy Act of 1974 (5 USC 552(a)) requires that prior to disclosure of personal information, applicants be provided a Privacy Act notification. Applicants must be informed that the purpose of the requested information is to establish eligibility for acceptance and accreditation in the special agent program. Routine uses of the information include making a determination for security clearance; verification of health; education; military training; ability to express oneself in written communication; and eligibility for continued assignment to criminal investigative duties. Although furnishing the information is voluntary, failure to furnish all or part of the information may result in a delay in processing the application or in non-selection for assignment to USACIDC.

c. While the applicant is preparing the application packet, the SAC, or their designated representative, will complete the following actions:

(1) Request and evaluate the following records checks:

(a) Local PMO/NCIC

(b) Local law enforcement checks

(c) US Army Crime Records Center

(d) Medical Record

(e) Community Counseling Center

(2) Conduct chain-of-command Interviews (first line supervisor to company commander or equivalent) to determine suitability. If an internship is needed, determine if unit will release the soldier for the internship program IAW Chapter 20. If qualified and released by his/her command for the intern program, the applicant may begin administrative duties within the CID office. Note that the applicant cannot perform internship functions, other than administrative duties until approved for entry into the internship program IAW Chapter 20.

d. Applicant Responsibilities. Initial actions are largely the responsibility of the prospective applicant. They must complete all forms, schedule and take all required tests, and compile a complete application packet. Instructions and necessary forms required to complete the packet are provided on the USACIDC Intranet and may be obtained from the local CID office. Applicants and interns will not be given user name and password access to the USACIDC Intranet. The application packet will consist of:

(1) Application cover memorandum, see Figure19-4.

(2) The Electronic Personnel Security Questionnaire (EPSQ) in paper and electronic (disk) form. This program provides an automated SF Form 86, Questionnaire for National Security Positions and 86-A (as required). This electronic form must be submitted as part of the packet for initiation of the SSBI, in accordance with AR 380-67. The applicant must also use the EPSQ validation program that checks this form for errors to ensure that the EPSQ is printed without errors, then signed and dated. If the applicant has a current Top Secret clearance based on a current SSBI (within five years), the EPSQ does not have to be submitted. The applicant must provide a memorandum of security clearance verification from the local security manager. The EPSQ will be forwarded with the application to HQUSACIDC for submission to DSS.

(3) A completed Applicant Background Questionnaire (Figure 19-5) and an Applicant Financial Questionnaire (Figure 19-6) and current (within last six months) credit history report. The Disclosure Form (Figure 19-7) must be completed by the applicant prior to obtaining the credit history report. The fee for the credit report will be funded with the CID unit's IMPAC card.

(4) Copies of the last two NCOERs, (if available).

(5) A list of service schools completed, course title, and date completed.

(6) One current copy of DA Forms 2A and 2-1 (Personnel Qualification Record, Parts I and II) or Enlisted Record Brief (ERB).

(7) Letters of appreciation, commendation, and recommendation in support of the application may be submitted at the option of the applicant. The absence of these letters may make it difficult to reach an equitable decision.

(8) A copy of a current DA Form 705, Army Physical Fitness Test (APFT) scorecard.

(9) A current body fat content (BFC) worksheet, if the applicant exceeds the screening table established in AR 600-9.

(10) Results of the Total Adult Basic Education (TABE) test; active component requirement only.

(11) Copy of the applicant’s stateside and military driver’s licenses.

(12) Written requests for waivers of standards must be submitted with the application with complete justification provided IAW paragraph 19-3i below.

(13) Other material deemed appropriate by the applicant.

(14) Unit Commander’s endorsement of soldier’s application cover memorandum IAW paragraph 19-3 d(1).

(15) Microfiche of the applicant’s Official Military Personnel File (OMPF), if available.

(16) One color photograph taken in civilian clothes (coat and tie, male; equivalent attire, female) in DA format.

(17) Official college transcripts from accredited institutions. Each applicant must obtain these documents at their own expense. If the policy of the college or university precludes the release of transcripts to the individual, the institution should be requested to forward the transcripts directly to the CG, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506. Comments to this effect should be included with the application. Additional credits acquired as a result of DANTES and CLEP examinations will also be considered. The Army American Counsel on Education Registry transcripts will not be considered in lieu of an official transcript. These course credits must be evaluated through an accredited institution and documented on an official transcript. Credits awarded for military training may not be duplicated on more than one transcript and forwarded for consideration. It is preferred that all credits be evaluated and consolidated on one official transcript by the institution where the applicant is currently enrolled.

(18) Results of local medical records screening documented on a DA Form 4254-R, Request for Private Medical Information (Figure 19-8).

e. Once the requirements of paragraph 19-3d have been met, the applicant will submit the application packet to the SAC. If there is a delay in obtaining items in paragraphs 19-3d(15) through (18), the application packet can be forwarded without them. These items can be forwarded at a later time under separate cover.

f. Upon receipt, the SAC, or their designated representative, will review the packet to ensure the applicant has provided all of the material required.

g. The SAC, or their designated representative, will review the EPSQ for completeness and any indication of adverse information, run the verification program, and resolve any errors.

h. The SAC, or their designated representative, will then add the following to the application packet:

(1) The applicant’s fingerprints on two copies of FD Form 258 (FBI U.S. DOJ Applicant Fingerprint Card (blue)).

(2) An autobiography, written at the time of interview in the applicant's own handwriting and prepared under the supervision of a USACIDC representative. The autobiography must be signed by the applicant and witnessed by the USACIDC representative to certify compliance with this provision.

(3) The SAC’s interviewer letter reporting that the interview was conducted and the results of the interview (Figure 19-9).

i. Waivers:

(1) Prerequisites may be waived at the sole discretion of the CG, USACIDC, or a designated representative. Waivers for the disqualifiers outlined in AR 195-3, will not be granted.

(2) Written requests for waivers of prerequisites must be submitted with the application with complete justification provided, including recommendations of intermediate commanders.

j. The SAC will mail the completed application packet IAW with paragraph 19-6 below.

19-4
Application Process for Warrant Officer Appointment

a. Individuals desiring appointment as a warrant officer, MOS 311A, must submit applications in accordance with AR 135-100 or NGR 600-101, as appropriate (see USAREC website www.usarec.army.mil for WO checklist). In addition to those items required in AR 135-100 or NGR 600-101, applications must include the following:

(1) Official college transcripts from an accredited institution, or acceptable college level testing programs. If college or university policy precludes the release of transcripts to the individual, the applicant should request that the transcripts be sent directly to the CG, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506, and include a comment to this effect with the application.

(2) Copies of the applicant's last three NCOERs (if not immediately available, the applicant will so state).

(3) Letters of recommendation from past and current USACIDC agent supervisors may be included.

(4) The application must receive formal endorsements through the applicant’s rating chain. Each endorser will provide a candid, dispassionate assessment of

the applicant's suitability and potential for success as a USACIDC warrant officer. The endorser must also provide recommendations pertaining to any waivers requested by the applicant.

b. Waiver Process

(1) Requests for waivers should be IAW AR 135-100 or NGR 600-101, as appropriate. Written requests for waivers must be submitted to HQUSACIDC with the application with complete justification provided, including recommendations of intermediate commanders.

(2) MOS 311A qualification standards may be waived at the sole discretion of the CG, USACIDC, or a designated representative.

(3) Years of active federal service may be waived at the sole discretion of the Office of the Deputy Chief of Staff, Personnel, HQDA.

(4) Moral waivers may be waived at the sole discretion of the Commander, Army Reserve Personnel Command (AR-PERSCOM).

19-5
Application Process for Civilian Investigator

Applicants for the Civilian Investigator Program, Series 1811, must submit their applications directly to the servicing Civilian Personnel Office (CPO) IAW information provided in position vacancy announcements. Applicants desiring additional information may inquire through HQUSACIDC, ATTN: CISP-CP, 6010 6th Street, Fort Belvoir, VA 22060-5506.

19-6
Forwarding Applications

a. Enlisted special agent applications will be forwarded directly to the Commander, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506, from the interviewing office.

b. Warrant officer applications.

(1) Applications from members of the Active Army for appointment as a warrant officer special agent will be sent through the appropriate USACIDC group commander to CG, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506 for approval/disapproval.

the next possible BSAC prior to receipt of the completed SSBI. If, upon review of the SSBI, information exists that warrants removal from the program, the individual may be processed for removal as outlined in Chapter 21 of this regulation.

19-8
Probationary Period

a. Accreditation of special agents is accomplished by the authority of the CG, USACIDC, through the Chief, Accreditation Division, USACIDC, upon graduation from the Basic Special Agent Course (BSAC).

b. All special agents will serve a probationary period of one year, beginning on the date of graduation from BSAC. Normal absences for leave or schools will not cause an extension of the probationary period unless of such duration that a comprehensive assessment of the probationary special agent's abilities cannot be made. Under exceptional circumstances where the probationary agent demonstrates proficiency commensurate with those of an accredited and well experienced agent, early accreditation may be requested through the chain-of-command and approved by the CG, USACIDC, under the same provisions as detained in paragraph 19-8b(4) of this regulation.

(1) All civilian special agents who are new to federal service will also serve a one year probationary period. Civilian special agents and forensic examiners will remain accredited for as long as they sustain the qualifications outlined in AR 195-3.

(2) Field commanders/SACs must ensure that probationary special agents are properly supervised and managed during the probationary period to ensure that a proper evaluation for continued USACIDC service can be made. Probationary special agents will not be placed in positions where they cannot be evaluated. Probationary special agents serving in overseas areas should be encouraged to extend their tour in order to complete their probationary period without interruption. Personnel assigned to USACIDC are stabilized in accordance with AR 614-5.

(3) If a special agent (active duty or reserve) is transferred during the probationary period, the losing commander will forward the monthly evaluation reports to the gaining commander and immediately notify the CG, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506. This will facilitate reporting completion of the probationary period.

(4) Termination of the probationary period will occur on the one year anniversary of graduation from the BSAC, unless the battalion commander determines that an extension is needed. Under no circumstances will the

probationary period be extended for more than six months. When the twelve month period has ended and the battalion commander, or in the case of USAR and NG USACIDC units, detachment commanders, determines that the probationary agent has fulfilled all probationary requirements, the commander will certify, in writing, that the probationary period has ended and the agent is fully qualified. The USACIDC commander will forward a memorandum through the chain of command to the CG, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506, documenting that the probationary period is ended (Figure 19-10). If the commander determines that an extension is needed, the commander will forward a memorandum through the group commander to HQUSACIDC notifying that they are initiating an extension to the probationary period. This notification will include the duration of the extension period and a copy of all probationary monthly evaluation reports received by the probationary agent to that date. Probationary monthly evaluation reports must continue to be prepared throughout the extension period. Upon completion of the extension, the commander will either terminate the probationary period or begin action to eliminate the agent from the program. Again, the commander will provide HQUSACIDC with notification of termination of the probationary period and provide a copy of the probationary reports prepared during the extension period. Commanders desiring to eliminate a probationary special agent during the normal probationary period may do so at any time IAW guidelines in Chapter 21 of this regulation.

19-9
Request for Return to Active Duty as a CID Agent

a. Individuals desiring to return to active duty as USACIDC agents must meet standards specified in AR 195-3, to include a current SSBI.

b. Qualified individuals will submit a written request to the Commander, USACIDC, ATTN: CISP-AC, indicating their prior term of service, current address, and telephone number, the name and contact information of a former CID supervisor, and the last two NCOER/OER received, if available.

c. The Accreditation Division will coordinate with the warrant officer or enlisted assignment manager, PERSCOM, to determine position availability.

d. Upon review of the applicant’s accreditation file, and satisfaction of the requirements of paragraph 19-4a if applicable, a memorandum of acceptance for reinstatement as a USACIDC agent will be forwarded to the applicant and the assignment manager by the Chief, Accreditation Division, HQUSACIDC.

e. Enlisted applicants, upon receipt of the memorandum of acceptance, will contact their local Army recruiter advising them of their desire to return to active

duty and provide the recruiter with the acceptance memorandum. A grade determination will be made by PERSCOM.

19-10
Release Process

The process governing agent misconduct, substandard performance, and accreditation review procedures is provided in Chapter 21, of this regulation.

19-11
Administration of the CIAF

a. The purpose of this section is to assign responsibility for initiating, maintaining, and controlling the CIAF. Additionally this section:

(1) Prescribes controls for filing data and documents in the CIAF.

(2) Prescribes documents authorized for filing in the CIAF.

(3) Prescribes filing instructions for adverse information.

(4) Enables the USACIDC to respond to allegations of prior agent misconduct and judiciary requests for agent misconduct information.

b. The objectives of this section are to:

(1) Apply equitable filing standards to all persons who have applied for and been accepted/accredited as a CID agent.

(2) Protect the rights of individuals and permit the HQUSACIDC to consider all relevant information when making acceptance/accreditation decisions and recommendations for appointment to warrant officer, MOS 311A or specialty programs.

(3) Ensure the availability of accurate, relevant, timely, and complete information for CID decision-makers.

c. The CIAF will be disposed of in accordance with AR 25-400-2.

19-12
Custodian of the CIAF

The Chief, Accreditation Division, is designated as the custodian of the CIAF. As such, the division chief may designate assistant custodians as required. The custodian is responsible for the initiation, maintenance, safeguarding, disposition, and release of information from the CIAF in accordance with this section.

19-13
Control of the CIAF

The CIAF unclassified data will be safeguarded as "For Official Use Only." No data within the CIAF will be released to agencies outside the USACIDC unless the release is consistent with this chapter, AR 25-55, chapter 20 (Freedom of Information Act) and AR 340-21 (Privacy Act), court order, and authorized by the DCSSPT, or other appropriate authority, as provided in paragraph 19-14 of this section.

19-14
Access To and Loan of the CIAF

a. The CIAF will not be forwarded or carried outside HQUSACIDC. The following individuals are authorized access to and loan of the CIAF:

(1) CG; DCO; Chief of Staff; DCSOPS; DCSSPT; Assistant DCSSPT for Agent Development; Command Sergeant Major, Secretary of the General Staff; Chief, Current Operations/Policy Division, HQUSACIDC; and MSC group/district commanders.

(2) CID Inspector General.

(3) CID Staff Judge Advocate.

(4) Accreditation Division personnel.

(5) Consideration boards conducted by HQUSACIDC as described in paragraph in Chapter 21.

b. All CID special agents will be granted access to their CIAF upon request. The custodian will ensure that no information protected by the Privacy Act is contained in the file prior to allowing access to the individual CID special agent for review within the division.

c. The CID HQ Form 488, File Review Log, will be utilized to record the identity of all individuals reviewing the CIAF.

d. Personnel authorized loan of the CIAF will ensure the CIAF is safeguarded and promptly returned to the Accreditation Division.

19-15
Initiation of the CIAF

The CIAF will be initiated by the CIAF custodian for military or civilians in the following circumstances:

a. Receipt of an application for acceptance as a CID special agent.

b. Receipt of a request for issue of badge and credentials as a civilian special agent or CID supervisor or USACIL examiner.

c. Upon issuance of a sequence number to civilian employees of the CID who are in investigative support positions.

19-16
Use of the CIAF

The primary use of the CIAF is to document an applicant's initial acceptance or non-acceptance into the CID program and, if accepted, the CID special agent's continued eligibility, placement and standing within CID. The CIAF may also be screened when considering CID special agents for the following:

a. Special assignments.

b. Elimination and disciplinary actions.

c. Advanced military and civilian schooling.

19-17
Documents Authorized in the CIAF

Only those documents specified in this chapter are authorized for filing in the CIAF.

a. In addition to any document properly filed in accordance with AR 640-10 in the Official Military Personnel File (OMPF), the Military Personnel Records

Jacket (MPRJ or Field 201 File) or the Career Management Individual File (CMIF), the following documents with allied papers will be filed in the CIAF:

(1) Applications, including all enclosures, for acceptance or accreditation in the CID program or any of its specialty areas.

(2) Standard Form 171/Optional Form 612/Resume.

(3) Job descriptions of civilian special agents, mobility agreements and any training agreement.

(4) Character or background investigation synopsis.

(5) Reports of investigation with supporting documents.

(6) Probationary evaluation reports.

(7) Recording data: Acceptance and accreditation data, including date of acceptance, accreditation, appointment, badge and credential number, and other data pertaining to the accreditation function.

(8) Civilian clothing allowance requests and approvals.

(9) Orders and Notification of Personnel Actions, including reassignment, reclassification, promotion, reduction and court-martial orders.

(10) Other documents as approved by the CG.

(11) Other data as included in Privacy Act systems notice, AR 340-21, A0190-30DAMO.

(12) ARB results.

b. Additionally, the following documents may be filed in the CIAF:

(1) Academic records and documents.

(2) Preliminary and commander’s inquiries with supporting documents together with any action taken by the command including copies of letters of concern, admonition, reprimand or counseling pursuant to in Chapter 21.

(3) Quality control data, including, but not limited to, commendatory memoranda, local and general memoranda as defined in this chapter, and unfavorable information with the CG's approval.

19-18
Forwarding of Documents for Inclusion in the CIAF

Except as provided in Chapter 21, the above documents should be forwarded by the commander or special agent-in-charge through the USACIDC MSC to HQUSACIDC, ATTN: CISP-AC, for inclusion in the CIAF. This requirement is in addition to and separate from other filing or destruction requirements pertaining to the U.S. Total Army Personnel Command (TAPC) sponsored personnel records.

19-19
Processing Local or General Memoranda

a. The provisions of AR 600-37 are generally applicable to memoranda of counseling, admonition, censure and reprimand intended to be filed in the CIAF. These memoranda will be given to an agent together with supporting documents and notice the commander intends to recommend filing in the CIAF. The agent will be given a reasonable opportunity to provide a written response. Documents intended for filing in the CIAF will be forwarded through the chain of command for a filing decision. Only the CG, USACIDC, has the authority to direct the filing of derogatory information in the CIAF.

b. Local memoranda of counseling or admonition will normally not be forwarded or filed in the CIAF. These memoranda may be retained at the writer's work place for not more than 2 years, or sooner upon permanent change of station (PCS) reassignment of the individual, at which time they will be destroyed.

19-20
Record Access Procedures

a. Requests for access to the CIAF from individuals should be addressed to: Director, Crimes Record Center (CRC), ATTN: CICR-FP, 6010 6th Street, Fort Belvoir, VA 22060. Written requests for information should contain the full name of the individual, current address, date of birth, and whether the individual has ever applied for the CID program, and, if so, year accepted, rejected, or eliminated.

b. The Chief, Accreditation Division is authorized to allow individuals to review their file. Personal visits to review the CIAF should be preceded by as much notice as possible to avoid unnecessary waiting or inconvenience. Visitors must present acceptable items of identification.

19-21
Challenging Record Contents

The rules and procedures used for challenging the contents of the CIAF or requesting amendment thereto will be the same as contained in AR 195-2, Chapter 2 of AR 340-21; and Chapter 21 of this regulation. Appeals for the removal of unfavorable information filed in official personnel files (MPRJ or OMPF) will be processed under AR 600-37, chapter 7.

Figure 19-1. Realities of the Investigative Profession

REALITIES OF THE INVESTIGATIVE PROFESSION

One frequent problem encountered among personnel selected for USACIDC duty is that many say they were unaware of the aspects of accepting duty in the agent career field. In some cases they indicated they would have reconsidered their decision to apply if they had known of the pressures associated with USACIDC duty. Below is a list of “realities” that are associated with USACIDC duty. These realities are divided into two categories. The realities in the first category are “part and parcel” to entry into the investigative profession. They would be present in any job whether in the U.S. Army or society at large. However, they also affect individuals volunteering for USACIDC duty. The second category involves realities that are associated strictly with USACIDC as part of the U.S. Army.

CATEGORY 1: REALITIES OF THE INVESTIGATIVE LAW ENFORCEMENT PROFESSION

1. Most of what we do is very routine--necessary paperwork, research, and documentation. In fact you will do more paperwork and writing in this career field than in most others in the Army, including administrative career fields.

2. No special favors go with your badge and credentials.

Use of USACIDC badge and credentials for other than official USACIDC business is strictly prohibited and will warrant disciplinary action.

3. Investigative work does not lend itself to a routine 8-to-5 duty day.

Irregular hours (overtime on weekends, nights, and holidays).

Long hours.

CID agents are often responsible for investigations from start to finish regardless of leave, night school, etc.

You will, on occasion, miss birthdays, anniversaries, and holidays with family and loved ones.

4. CID agents are expected to perform across the spectrum of the USACIDC mission responsibility, e.g., criminal, fraud, drug and protective service missions. While many opportunities exist, at times, specialization is limited.

CID agents are required to handle sources (informants). Those personnel who feel uncomfortable with recruitment or management of human sources to collect

information on others should strongly reconsider their decision to seek a career as an USACIDC special agent.

5. A CID agent's job is to seek out and document the facts for a commander or appropriate authority (United States Attorney, district attorney, etc.) to make a decision.

Unsolved and unadjudicated cases cause frustration.

Investigations have to satisfy the requirements of USACIDC as well as that of the installation commander or other prosecutive authority. We have many requirements to meet federal law and investigative sufficiency that may not be needed by the local prosecution authority.

Actions of the CID agent are continually scrutinized for legal sufficiency and adherence to USACIDC and Army policies. We are required to prove allegations "beyond a reasonable doubt," which is extremely difficult, if not impossible, in some cases.

6. Family stress.

CID agents frequently cannot discuss their work with family members

Potential for harassment of family members because of agent status.

Duty requirements frequently interfere with family social and recreational activities.

Family members should know that the agent will carry and use firearms and could be exposed to dangerous situations.

Spouses often have to care for family alone without the agent's help for extended periods of time due to TDY, PCS, and other priority mission requirements.

Without question, family relationships will be stressed. CID agents and their spouses must be prepared to deal with this effectively by using, when necessary, the various organizational, religious, medical, and social resources available in the Army and civilian communities.

Does the spouse fully support the applicant's request for USACIDC duty?

7. Agent stressors ("no one ever calls with good news").

Often being second guessed and possibly criticized. Constant emphasis to reach the highest investigative standards in all cases, no matter how seemingly mundane or trivial the investigation.

Twelve-month probationary period, extended if necessary.

Suspenses, suspenses, suspenses.

Sensitive, classified, and compartmented information. ;

May be ostracized by peers and other members of society.

Handling and control of human sources (informants).

Narcotics subculture.

Duty agent--you have to be there when you're needed regardless of time: day, night, weekends, holidays

Use of lethal weapons.

Child abuse investigations.

Autopsies--observe and assist.

Some investigations may be extremely unpleasant, especially violent crimes.

Seemingly always too much to do and not enough time to do it all, and under pressure throughout.

CATEGORY 2: USACIDC AS PART OF THE ARMY

1. USACIDC's role is providing battle field support. This priority will at times adversely affect your ability to complete a myriad of other tasks to include high priority criminal investigations.

You are a CID agent with deployable skills in support of the Army's mission first, a criminal investigator second.

You will probably deploy at least once, if not more, during your USACIDC career.

USACIDC's average deployment is 180 days.

You will probably have at least one, if not more, short tour assignments (possibly to remote areas), during your USACIDC career.

2. Mission requirements cause personnel shortages that cannot be compensated through other Army or USACIDC resources.

Long-term TDY to meet mission needs.

Short notice TDY or PCS to meet mission needs.

Absence of one special agent could effectively render some units 1/2 or 2/3 manned.

3. US Army requirements (military special agents):

Must maintain both uniforms and civilian clothes.

Must satisfy requirements for promotion.

No special quotas for promotion in USACIDC.

Remote overseas tours.

Standard US Army assignment selection used in USACIDC.

Could be assigned to high-cost areas with no Army facilities available.

Must maintain APFT and AR 600-9 standards.

I have read and understand the above negatives associated with special agent duty in USACIDC.

_____ _____
(Applicant's Signature) (Date)

Figure 19-1. Realities of the Investigative Profession

Figure 19-2. CID Application Checklist
CID Application Checklist

The following items are part of the application submitted by the applicant to become a CID agent:

1. Application cover memorandum. (Figure 19-4)

2. A list of service schools completed, course title, and date completed.

3. One current copy of DA Forms 2A and 2-1 (Personnel Qualification Record, Parts I and II) or Enlisted Record Brief (ERB).

4. Standard Form 86 with two FD Forms 258.

5. DA style photo in business attire

6. Handwritten autobiography

7. Statement from USACIDC interviewer relative to interview results

8. Official College Transcripts

9. Letters of recommendation/commendation

10. A copy of a current DA Form 705, Army Physical Fitness Test Score Card (APFT). A current body fat content worksheet, if the applicant exceeds the screening table established in AR 600-9, if required.

11. TABE test results

12. Microfiche copy of current OMPF, if available.

13. A completed Applicant Background Questionnaire (Figure 19-5), an Applicant Financial Questionnaire (Figure 19-6), and the Disclosure Form (Figure 19-7).

14. Copies of last two NCOERs, if available.

15. Copy of the applicant’s stateside and military driver’s licenses.

16. Written requests for waivers of standards must be submitted with the application with complete justification.

17. Unit Commander’s endorsement of soldier’s application cover memorandum.

18. Documentary evidence of current education level in the form of official college transcripts from accredited institutions. Each applicant must obtain these documents at their own expense. If the policy of the college or university precludes the release of transcripts to the individual, the institution should be requested to forward the transcripts directly to the CG, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506. Comments to this effect should be included with the application.

19. Results of the local medical records screening documented on the DA Form 4254-R. (Figure 19-8)

20. Other material deemed appropriate by applicant.

Figure 19-2. CID Application Checklist

Figure 19-3. Authorization for Release of Information
Authorization for Release of Information

Carefully read this authorization to release information about yourself, then sign and date in ink.

PRIVACY ACT STATEMENT: Privacy Act of 1974 requires that each individual asked to provide information be advised of the following:
a. AUTHORITY: DoD Directive 5105.42 and 5 U.S.C. 301.
b. PURPOSE: This information is being requested to obtain information that will assist USACIDC officials in determining your suitability for a position in USACIDC.
c. ROUTINE USES: This information will be provided to and maintained by USACIDC. It may be furnished to accredited DoD agencies, accredited federal agencies, and law enforcement agencies for their official use.
d. VOLUNTARY DISCLOSURE: The disclosure of personal information to USACIDC is voluntary. However, if you do not desire to supply information, USACIDC may be unable to conduct a complete investigation and adjudicating officials may be unable to determine your suitability for a position with USACIDC.

I authorize any CID agent or other duly accredited representative of the USACIDC conducting my pre-acceptance investigation, to obtain any information relating to my activities from individuals, schools, residential management agencies, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, collection agencies, retail business establishments, or other sources on information. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, disciplinary, employment history, criminal history record information, and financial and credit information.

I further authorize any CID agent or any duly accredited representative of the USACIDC conducting my pre-acceptance investigation to obtain information from financial institutions, medical institutions, hospitals, health care professionals.
I authorize custodians of records and other sources of information pertaining to me to release such information upon request of the agent or any other accredited representative of the USACIDC regardless of any previous agreement to the contrary.

I understand that the information released by record custodians and sources of information is for official use the USACIDC only for purposes of determining eligibility for acceptance into USACIDC. Copies of this authorization that show my signature are as valid as the original release signed by me. This authorization is valid for three (3) years from the date signed or upon determination of my non-suitability for acceptance into USACIDC, whichever is sooner.

_____ _____

(Signed) (Dated)

Figure 19-3. Authorization for Release of Information

Figure 19-4. Application Cover Memorandum
Application Cover Memorandum

LETTERHEAD

XXXX-XX DATE

MEMORANDUM THRU Commander, 49th Military Police Company, Fort Bravo, CA 90505

FOR Commander, U.S. Army Criminal Investigation Command, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506

SUBJECT: Application for Acceptance as a USACIDC Agent

1. In accordance with provisions of AR 195-3, I request acceptance as a USACIDC special agent.

2. The following information is submitted voluntarily. I understand that in accordance with the Privacy Act (5 USC 552(a)) this information is solicited to facilitate the determination of my eligibility and ensure accuracy of information, which may be acquired during the processing of this application. I understand that the authority to solicit this information is 10 USC 3012(g) and that my failure to provide the required information may result in delay in processing and/or non-selection for the USACIDC program.

a. I am a United States Citizen by (birth)(naturalization).

b. I have no record of mental, emotional disorders, including pathological personality disorders as determined by the results of medical records screening.

c. I believe that a single scope background investigation will establish that I have favorable character, integrity, loyalty, reputation, sobriety, discretion, and stability.

d. I (do) (do not) have a record of unsatisfactory credit.

e. I (have) (have not) been tried by neither civil court nor arrested/apprehended for any offense (if affirmative explain in detail).

f. I (have) (have not) been tried by summary, special, or general court-martial (If affirmative explain in detail).

g. I am XX years old.

h. My physical profile is 111221 (Your medical records contain this information). Date of my latest Army Physical Fitness Test (APFT), 1 Jul XX; score: 300 Pass/Fail. My height is 6'2"; my weight is 165 lbs. I currently meet the standards of AR 600-9. (If the applicant exceeds the screening table weight a complete signed current body fat content worksheet will be attached.)

i. I (do) (do not) have normal color vision. (If the applicant does not have normal color vision, a physician must confirm that the individual can differentiate between green, red, and amber.)

k. My GT score is .

j. I have XX years of military service.

l. I (have) (have not) been granted a waiver for enlistment.

m. I (do) (do not) have a record of time lost under Section 972, Title 10, USC.

n. I (am) (am not) qualified as a military policeman (MOS 95B). (If not, the CID Forms 120-E-R, documenting completed intern training, must be enclosed.)

o. My primary MOS is XXAXX.

p. My marital status is (married/divorced/legally separated).

q. The date of my current enlistment and period of enlistment is 23 May XX, 5 years.

r. My DEROS (or date of return from last overseas tour, and place) is 22 Jan XX, Frankfurt, Germany.

The date of my last permanent change of station is 22 Jan XX.

s. I have acquired a total of XXX college semester hours and hold a (AA, AS, BA, BS, if applicable) degree in _____.

t. Should I be accepted for participation in the Criminal Investigation program, I will extend, enlist, or reenlist, if necessary, to meet the three year retention requirement, IAW AR 614-200.

u. I (do) (do not) have a valid current driver's license from the State of _____, #_____, expiration date_____.

14 Encls *JOHN SMITH*
1. List of service schools SGT, 429-46-1234

completed 49th MP Company

2. DA Forms 2 and 2-1 / ERB
3. Standard Form 86 and two FD Forms 258
4. Photo
5. Autobiography
6. Stmt from USACIDC interviewer relative to disposition of interview results
7. Official College Transcripts
8. Letters of recommendation/commendation
9. Copy of APFT, BFC (if applicable)
10. TABE results
11. Microfiche copy of current OMPF
12. Copies of NCOERs
13. DA Form 4254-R
14. Background and financial questionnaires and Disclosure Form
15. Other material deemed appropriate by applicant (list individually)
16. CID Forms 120-E-R (if applicable)

Figure 19-4. Application Cover Memorandum

Figure 19-5. Applicant Background Questionnaire

USACIDC APPLICANT BACKGROUND QUESTIONNAIRE

PRIVACY ACT STATEMENT: The Privacy Act of 1974 requires that each individual asked to provide information be advised of the following:
a. AUTHORITY: DoD Directive 5105.42 and 5 U.S.C. 301.
b. PURPOSE: This information is being requested to obtain information that will assist USACIDC officials in determining your suitability for a position in USACIDC.
c. ROUTINE USES: This information will be provided to and maintained by USACIDC. It may be furnished to accredited DoD agencies, accredited federal agencies, and law enforcement agencies for their official use.
d. VOLUNTARY DISCLOSURE: The disclosure of personal information to USACIDC is voluntary. However, if you do not desire to supply information, USACIDC may be unable to conduct a complete investigation and adjudicating officials may be unable to determine your suitability for a position with USACIDC.

INSTRUCTIONS: Please be entirely honest in answering this questionnaire. The fact that you might have had problems in your background, such as arrests, use of drugs, excessive drinking, mental problems, being fired from positions, or that there may have been accusations against your honesty or moral behavior, does not necessarily mean that your application for USACIDC duty will be disapproved. The authorities who make decisions based on information in your application look at the “whole person.” They weigh unfavorable information against favorable information and the individual’s truthfulness. However, if you fail to accurately disclose relevant information about your background or past behavior, and we subsequently uncover this information, your lack of truthfulness and failure to be candid or straightforward, will be an additional factor considered by the decision-making authorities. This questionnaire is only part of the broader inquiry that we will conduct as you successfully complete the various phases of USACIDC recruitment. In order to enter into USACIDC, you must undergo an extensive background investigation. Such an investigation will include checks of criminal agencies, reviews of education and employment records, and interviews of people who know you both at work and where you live. It will also explore, in-depth, the answers you provide on this questionnaire.

Answer all questions by circling either YES or NO. **Explain YES answers to questions 3 through 22 in REMARKS below.** You may be requested to provide additional information after completing the questionnaire or at a later date.

1. Do you understand the importance of being entirely honest when answering these questions? YES / NO

2. Are you and all members of your immediate family U.S. citizens?
YES / NO

3. Would your past actions result in others characterizing you as indiscreet, unstable, or of questionable character?
YES / NO

4. Have you ever been involved in deviant sexual behavior, such as child sexual abuse? YES / NO

5. Are there any incidents in your life, which could subject you to blackmail, e.g., extramarital affairs, undetected theft, fraud, or embezzlement? YES / NO

6. Do you have a history of excessive or habitual use of alcohol or any alcohol-related incidents that involved law enforcement authorities or caused personal or professional problems? YES / NO

7. Do you have a history of being a drug user, drug addict, drug supplier, or casual drug user? YES / NO

8. Have you ever experimented with any drugs, including marijuana?
YES / NO

9. Have you ever participated in a drug rehabilitation program because of your drug involvement or alleged drug involvement? YES / NO

10. Have you ever been arrested, detained, or charged with a criminal offense, had charges dropped, or been advised that no record would be made of an incident? YES / NO

11. Have you ever been arrested or charged with driving under the influence or driving while intoxicated or had such initial charges reduced to lesser charges?
YES / NO

12. Have you ever had any administrative or disciplinary action taken against you, either as a civilian or while servicing in the military? YES / NO

13. Have you ever been convicted by a military court or been the subject of a criminal investigation conducted by a military investigative agency?
YES / NO

14. Have you ever been punished under Article 15 of the Uniform Code of Military Justice? YES / NO

15. If married or previously married, does your spouse or do your ex-spouses have criminal records or any problems that may surface during an extensive background investigation? YES / NO

16. Have you ever been seen by mental health officials, counselors, or family advocacy officials to include counseling for marital problems or grief? YES / NO

17. Do you have a history of nervous disorders or anxiety reactions? YES / NO

18. Do you have a history of mental illness? YES / NO

19. Do you have any reason to think that anyone would believe you to be disloyal to the United States? YES / NO

20. Have you ever been approached to engage in espionage or sabotage against the United States? YES / NO

21. Have you ever engaged in espionage or sabotage against the United States? YES / NO

22. Do you have any unauthorized contact with representatives of a foreign government? YES / NO

23. Have you ever been approached to give or sell any classified or unclassified material to unauthorized persons? YES / NO

24. Are you now or have you ever been a member of any organization, association, movement, group, or combination of persons that:

(a) Advocates the overthrow of the American constitutional form of government, YES / NO

(b) Advocates or approves the commission of acts of force, violence, coercion, or intimidation to deny persons their rights under the Constitution of the United States YES / NO

(c) Seeks to alter the form of government of the United States by force, violence, or other unconstitutional means, or YES / NO

(d) Advocates or engages in the disruption or halting of US government activities through force, violence, or infiltration of the government service? YES / NO

25. Do you have anything or anyone in your background that may present a credibility problem during our background investigation to include people who are upset or angry with you (coworkers, neighbors or supervisors, etc.)? YES / NO

REMARKS (Use bond paper if you need additional space.)

I have answered all questions in this Background Questionnaire to the best of my knowledge and ability. I have not intentionally omitted or provided any incorrect or misleading information.

_____ _____
(Applicant's Signature) (Date)

Figure 19-5. Applicant Background Questionnaire

Figure 19-6. Applicant Financial Questionnaire

APPLICANT FINANCIAL QUESTIONNAIRE

PRIVACY ACT STATEMENT: Privacy Act of 1974 requires that each individual asked to provide information be advised of the following:
a. AUTHORITY: DoD Directive 5105.42 and 5 U.S.C. 301.
b. PURPOSE: This information is being requested to obtain information that will assist USACIDC officials in determining your suitability for a position in USACIDC.
c. ROUTINE USES: This information will be provided to and maintained by USACIDC. It may be furnished to accredited DoD agencies, accredited federal agencies, and law enforcement agencies for their official use.
d. VOLUNTARY DISCLOSURE: The disclosure of personal information to USACIDC is voluntary. However, if you do not desire to supply information, USACIDC may be unable to conduct a complete investigation and adjudicating officials may be unable to determine your suitability for a position with USACIDC.

INSTRUCTIONS: Please be entirely honest in answering this questionnaire. The fact that you might have had financial problems in your background does not necessarily mean that your application for USACIDC duty will be disapproved. The authorities who make decisions based on the information in your application look at the “whole person”. They weigh unfavorable information against favorable information and the individual’s truthfulness. However, if you fail to accurately disclose relevant information about your background or past behavior, and we subsequently uncover this information, your lack of truthfulness and failure to be candid or straightforward with us will be an additional factor considered by the decision-making authorities. This questionnaire is only part of the broader inquiry that we will conduct as you successfully complete the various phases of USACIDC recruitment. To enter USACIDC you must undergo an extensive background investigation. Such an investigation will include checks of criminal agencies, reviews of education and employment records, and interviews of people who know you both at work and where you live. It will also explore, in-depth, the answers you provide on this questionnaire.

Answer all questions by circling either YES or NO. ***Explain, in REMARKS below, any YES answers to questions 6 through 11.*** You may be requested to provide additional information after completing this questionnaire or at a later date.

1. Do you understand the importance of your being entirely honest in answering these questions? YES / NO

2. Are you currently employed off duty? YES / NO

3. Do you rely on off-duty employment to meet your financial obligations? (USACIDC restrictions, overtime, TDY, PCS, etc., could impact this.)
YES / NO

4. Is your spouse employed? YES / NO

5. Do you rely on your spouse's employment to meet your financial obligations?
YES / NO

6. Have you ever experienced financial difficulties? YES / NO

7. Do you have any reason to believe that there is any unfavorable credit information about you on record with any credit bureau, business, or court?
YES / NO

8. Has your financial situation ever been negatively affected as a result of divorce, separation, child support, etc.? YES / NO

9. Have you ever filed for bankruptcy or been involved in civil court action regarding financial matters? YES / NO

10. Do you think you are currently living beyond your means? YES / NO

11. Do you think an assignment to USACIDC will hurt your ability to meet your financial obligations? YES / NO

REMARKS (Use bond paper if you need additional space.)

I have answered all questions in this Financial Questionnaire to the best of my knowledge and ability. I have not intentionally omitted or provided any incorrect or misleading information.

_____ _____
(Applicant's Signature) (Date)

Figure 19-6. Applicant Financial Questionnaire

Figure 19-7. Disclosure Form

UNITED STATES ARMY
HEADQUARTERS, CRIMINAL INVESTIGATION COMMAND

Disclosure and Authorization
Pertaining to Consumer Reports
Pursuant to the Fair Credit Reporting Act

This is a release for the Department of the Army Criminal Investigation Command (USACIDC) to obtain one or more consumer /credit reports about you in connection with your application to become an Agent with CID or in the course of your employment with USACIDC. One or more reports about you may be obtained for employment purposes, reassignment, retention or access to classified information.

I, _____, hereby authorize the United States Army Criminal Investigation Command (USACIDC) to obtain such reports from any consumer credit reporting agency for employment or security purposes.

This authorization will be valid until termination of my affiliation with the Federal Government. Photocopies of this authorization that show my signature are as valid as the original release signed by me.

SIGNATURE

_____

Social Security Number

Date Of Birth

Street Address Apt Number

CITY STATE ZIP CODE

_____

Current Military Assignment

Privacy Act Statement
Section 6311 of Title 5, United States Code, authorizes collection of personal information, to include your social security number. The primary purpose of the requested information is to establish an applicant's eligibility for acceptance and accreditation in the CID Program or continued assignment to criminal investigative duties. Additional disclosure of the information may be made to a Federal agency when conducting an investigation for employment or security reasons. Furnishing the social security number, as well as other data, is voluntary, but failure to do so may delay or prevent action on the application.

Figure 19-7. (Disclosure Form)

Figure 19-8. Results of Medical Record Screening

Figure 19-8. Results of Medical Record Screening

Figure 19-9. SAC interview Checklist and Memorandum

SAC Interview Checklist and Memorandum

Interview and Interviewer's Responsibility for Processing Personnel for Acceptance as a USACIDC Agent

1. When an interview is required An interview of each individual is required prior to submission of an application for acceptance as a USACIDC agent. It serves to develop information essential in determining the applicant's suitability as a USACIDC agent.

2. Interviewer

a. An interviewer is a detachment sergeant, operations officer, SAC of a resident agency, SAC of a branch office, USACIDC field office commander, USACIDC district commander, USACIDC detachment commander, USACIDC group commander, or a field grade officer assigned to HQ, USACIDC in an operational position. The final interview will be conducted according to Chapter 19, and the person conducting the final interview will sign the Statement of Interview (Figure 19-11).

b. The checklist in Figure 19-12 will be used to plan the interview. As each area is covered, it should be checked. On completion of the processing procedures, the list will be attached as an enclosure to the letter of transmittal forwarding the interviewer's evaluation of the applicant to the Commander, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506.

3. Interview

a. The detachment sergeant or a designee will conduct an initial screening of the individual's application to determine whether the applicant meets the prerequisites of AR 195-3 and paragraph 4, Chapter 19. If the applicant does not meet the waiverable requirements, the detachment sergeant will inform the individual of such failure and furnish instruction on the procedures for requesting the waivers that must accompany the application. If an applicant does not meet the nonwaiverable requirements, the detachment sergeant will inform the individual that the application cannot be accepted and terminate the interview. The interviewer will screen the applicants Military Personnel Records Jacket (field file) and medical records (with the assistance of medical personnel or by medical personnel) to identify any derogatory information that would affect USACIDC acceptance or subsequent issuance of a top-secret security clearance. Results of this screening will be shown in the interviewer's statement. The interviewer will also discuss the applicant's performance with the applicant's immediate supervisors/chain of command. Derogatory information will be

discussed with the applicant and reported in the USACIDC interviewer's statement.

b. The interviewer will ---

(1) Ensure that the individual has been given a proper Privacy Act notification as specified in paragraph 7a.

(2) Inform eligible applicants concerning MOS 95D duties and responsibilities of a CID agent. The interviewer will not make any commitment for the acceptance of the individual or any assignment of the applicant into the USACIDC Program.

(3) Determine whether the applicant is still interested in applying for acceptance as a USACIDC agent. If the individual is still interested, the interviewer will conduct an interview and outline to the applicant the assignment, duty requirements, and retention criteria of all USACIDC agents.

(4) Ensure the applicant is aware that acceptance by the CG, USACIDC, is not assurance that he or she will remain a USACIDC agent. Also, ensure the applicant understands he or she must successfully complete the prescribed course of instruction and the probationary period after graduation from the Basic Special Agent Course.

c. During the interview at the USACIDC office, the detachment sergeant will have the applicant prepare a handwritten autobiography stating the reason for applying for acceptance as a USACIDC agent. The applicant will also provide a brief synopsis of past employment, education, and experience. The applicant must be informed that the purpose of the composition is to determine the applicant's penmanship ability and written communication skills in the English language. A poorly written autobiography could contribute to the disapproval of the application. The following areas must be included:

(1) Level of formal education.

(2) Major field in which the applicant has been employed (for example, police work or clerical).

(3) A brief description of duties performed.

(4) Length of time engaged in each field.

(5) Highest degree of responsibility assumed in each position.

(6) Description of major incidents in life that have affected the applicant's personality, character, or outlook on life in general.

e. The applicant and the detachment sergeant or other USACIDC representative will both sign the autobiography to certify that it was handwritten by the applicant while at the USACIDC office.

4. Conduct of the final interview

a. The final interview should provide an opportunity to--

(1) Observe and evaluate the applicant closely.

(2) Elicit information that can only be obtained through an informal discussion with the applicant to explore the following areas fully:

(a) Family background.

(b) Personal problems that may limit the usefulness of the applicant in investigative duties.

(c) Any foreign language ability, how acquired, and degree of proficiency.

(d) Financial responsibility.

(e) Courses of study, technical training, and other skills or hobbies that improve the applicant's potential for investigative duties.

(f) Knowledge or interest in police and legal matters.

(g) Applicant's reasons and basic motivation for applying for investigative duties.

(h) Any other subjects deemed essential by the interviewer to evaluate the applicant and to complete the statement of interview.

b. The interview must be conducted in a manner to provide a basis for properly estimating personality traits described in (1) and (2) below and appraising the applicant in order to determine other qualifications set forth in (3) through (5) below.

(1) Motivation and reasons for applying for MOS 95D, poise, mental alertness, sincerity, ability to think quickly, oral expression, personality, and maturity.

(2) The following qualities and attitudes:

(a) Neatness.

(b) Good posture.

(c) Good stature and physique.

(d) Proper demeanor.

(e) Proper attitude.

(f) Common sense. Is quick to grasp a situation.

(3) The following education skills:

(a) Ability to write in the English language.

(b) Oral communication skills in the English language.

(4) The following moral views:

(a) Definite ideas of right and wrong in personal and public life.

(b) A sense of personal responsibility.

(c) Religious and racial tolerance.

5. Statement of interview: The interviewer will prepare a statement of interview that will include the information indicated in the format shown in Figure 19-8. The statement will be annotated "For Official Use Only". Information relating solely to the character, integrity, or suitability of the applicant will normally be afforded the protective covering of "For Official Use Only".

6. Action required by interviewer: The following action will be taken by the interviewer:

a. Assist the applicant, as necessary, in preparation of the request for waivers of prerequisites, when determination has been made that waivers are required.

b. Review items on the checklist to ensure that all requirements have been fulfilled.

c. After all requirements have been completed and the interviewer has determined that the applicant is administratively qualified for acceptance into MOS 95D, with or without waivers, prepare a statement of interview.

Figure 19-9. SAC Interview Checklist and Memorandum

Figure 19-10. Termination of Probation

Termination of Probation

Letterhead

CIXX-XX (MARKS #) DATE

MEMORANDUM THRU

Commander, 3d Military Police Group (CID), USACIDC, Forest Park, GA 30297

FOR Commander, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506

SUBJECT: Termination of Probation

1. Sergeant Doe satisfactorily completed his probationary period on 1 Jan XX.

2. Enclosed is the Basic Special Agent Course (BSAC) diploma and the final evaluation report (CID Form 120-E-R) which includes the results of all monthly evaluation reports prepared previously. Also attached (if applicable in the event a waiver was granted) is an update of SGT Doe's civilian education obtained since his acceptance into the USACIDC program.

2 Encls
1. Copy of BSAC Diploma
2. CID Form 120-E-R

JOHN F. SMITH
LTC, MP
Battalion Commander

Figure 19-10. Termination of Probation

Figure 19-11. Statement of Interview

Letterhead

CIRB-ZB XX April XXXX

MEMORANDUM FOR Commander, U.S. Army Criminal Investigation Command, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506

SUBJECT: Statement of Interview

1. In compliance with AR 195-3, on XX Apr XX, SPC George A. Custer, 000-00-0000, 123d Military Police Company, Fort Hamilton, NY 00021-4352, an applicant for acceptance as a CID agent in the U.S. Army Criminal Investigation program, was interviewed. His personnel and medical records were screened with (negative results) (the following information developed:). The applicant's immediate supervisor/chain of command were interviewed and they reported the applicant was (performing well) (was not performing because:).

2. I interviewed the applicant concerning the following points: family background, appearance, education, demeanor, moral views and character, integrity, discretion, financial responsibility, technical training, skills and hobbies that would enhance the applicant's potential for investigative duties, previous leadership positions held, basic motivation for applying for investigative duties

3. (Reason applicant desires acceptance into MOS 95D as a CID agent.)

4. The following adverse or derogatory information was obtained concerning those items listed in paragraph 2 above: (If no adverse or derogatory in formation was obtained state None).

5. Waivers. (Outline the prerequisites for which a waiver is requested and the interviewer's recommendation concerning approval or disapproval. If no waivers are necessary, state this fact.)

6. Recommendation. (Include in this paragraph the interviewer's recommendation concerning the applicant's acceptability into the Criminal Investigation Program.)

JIMMY J. RENO
CW4, USA
Special Agent in Charge

Figure 19-11. Statement of Interview
Figure 19-12. Interview Checklist

Interview Checklist

1. Give the applicant a copy of the Privacy Act Statement to read before the interview.

2. Give the applicant a complete orientation.

3. Answer all questions posed by the applicant.

4. Assist the applicant in preparation of the documentation required for the single scope background investigation (SSBI).

5. Have the applicant prepare a short handwritten autobiography for inclusion with the application. Be sure to certify its preparation under CID supervision.

6. Check personnel/medical records and discuss applicant's performance with the applicant's immediate supervisors/chain of command. Be sure that the records examined and supervisor's discussion are covered in the Statement of Interview.

7. Conduct the personal interview.

8. Prepare the Statement of Interview (below).

9. Do not make any promise concerning acceptance of the applicant into CID or any future duty assignments.

10. Determine for yourself that the applicant you interviewed and recommended for acceptance into the criminal investigation program possesses all the traits, skills, and characteristics desired of CID agents.

11. Advise the applicant that you should be contacted immediately if a decision is made to withdraw the application or disqualifying facts become known.

12. Advise the applicant to contact you immediately if the applicant changes their official address due to PCS or extended TDY.

13. Advise the applicant to contact you to check on the status of their application, and not to personally contact the Accreditation Division, HQUSACIDC.

Figure 19-12. Interview Checklist

CHAPTER 20

20-1
Purpose

This chapter prescribes policy for the attachment and training of prospective USACIDC applicants who lack the required law enforcement experience IAW AR 195-3, Acceptance, Accreditation, and Release of United States Army Criminal Investigation Command Investigative Personnel, 22 Apr 87. It is intended to formalize the process for attachment of personnel who have no law enforcement experience to CID field elements for training, which will serve as a substitute and qualify the applicant for a waiver IAW AR 195-3.

20-2
Applicability

This policy applies to all Active Component USACIDC field elements. Reserve Component USACIDC personnel and/or field elements will not have Intern Programs.

20-3
Applicant Eligibility/Acceptance

a. Prospective CID applicants who meet all the prerequisites for acceptance as a CID special agent as outlined in AR 195-3, except for law enforcement experience, may apply to their local CID field element for acceptance as a criminal investigation intern.

b. Prior to requesting acceptance into the intern program, the application requirements outlined in Chapter 19, paragraph 19-3, will be completed. No request for acceptance into the intern training program will be processed until the required local records checks and the EPSQ have been completed.

c. The SAC will forward the request for intern training to the Accreditation Division, USACIDC, as shown at Figure 20-1. This will be utilized as a cover memorandum to the basic application for acceptance.

d. If qualified and released by their command, the applicant may begin administrative duties within the CID office. At this stage, the applicant has not yet been approved for entry into the intern training program and cannot perform intern functions, other than administrative duties. The CID SAC will immediately notify the Accreditation Division, USACIDC, via e-mail of the attachment of intern, and forward a copy of his/her application (Figure 20-1) to the Accreditation Division. The Accreditation Division will then effect coordination with PERSCOM,

and if the MOS branch release is favorably considered, will notify the CID field element that the intern is approved for entry into the intern training program.

e. Once approved by HQUSACIDC for intern training, soldiers will train at a CID field element for 6 months. Not later than the mid point of the intern training program, the SAC's recommendation regarding the intern's CID application, will be forwarded to the Accreditation Division, USACIDC. The required monthly intern evaluation reports, as well as, the final evaluation report will be completed IAW paragraph 20-7.

f. No internship will exceed 6 months without the prior approval of the battalion commander. Internships that exceed 9 months must be approved by the group commander.

20-4
Applicant Attachment

a. CID commanders and SACs will facilitate the attachment of applicants for the CID intern program through coordination with the applicant's unit commander. The applicant and the applicant's commander must be made aware of the risks involved when using soldiers outside their assigned MOS.

b. Applicants approved for CID intern training must be attached to the sponsoring CID field element on attachment orders for duty only. The applicant's commander will retain all administrative, judicial, and current MOS training responsibilities. Applicants who are determined to be unsuitable for reasons of misconduct, background history, or lack of aptitude for continued CID duty will be returned to their unit for duty in their original MOS. The SAC will immediately notify the Accreditation Division, of this action. The decision of a SAC to terminate intern training and return a soldier to his/her unit for misconduct, demonstrated poor performance, or lack of aptitude for CID duties is not subject to appeal. CID interns, who are determined to be unsuitable based upon information developed by the SSBI, will be returned to their unit. The SAC will send a written memorandum detailing the reasons for the applicant's return to the applicant's commander with a copy furnished to the Accreditation Division.

c. Applicants serving in CID intern training positions may voluntarily withdraw their CID application without prejudice. The SAC will immediately notify the Accreditation Division when this occurs.

20-5
Applicant Training

a. CID interns will train under the direct supervision of an accredited CID agent. The supervising agent will be personally responsible to train the intern in the full range of investigative duties encountered by CID field agents. Rotation of interns among investigative areas, i.e., general crimes, economic crime, and drug suppression, may be advisable depending on the size of the field element and the volume of cases. Subject to the limitations of paragraph 20-6, the emphasis for CID interns should be general crimes, with exposure to receiving complaints, responding to reported incidents, crime scene processing, evidence collection procedures, crime scene sketching, photography, attendance at post-mortem examinations, interviews and interrogations, report writing, the criminal intelligence process, use of investigative equipment, investigative authority and responsibility, and conflict resolution. Administrative duties will not be considered or accepted as intern training. Intern training will be documented monthly on the CID Form 120-E-R, Probationary Agent Monthly Evaluation Report. A terminal evaluation will be forwarded with the commander/SAC certification.

b. Consideration should be given to the number of interns assigned to a field element at any given time. One intern per accredited/non-probationary/non-apprentice case agent is the maximum allowed. If the interns are noncommissioned officers (NCOs), they need to be evaluated and counseled accordingly. For the purpose of NCO evaluation reports, the intern's principal duty title should be reflected as "Criminal Investigation Intern" and duty MOSC "95D00."

c. CID interns should be fully integrated into the field element's training schedule. Interns should be required to attend scheduled training and common task training. Interns should be encouraged to attend off-duty college level criminal justice courses and to enroll in the criminal investigation correspondence course, as well as other related correspondence courses offered by the Army Institute for Professional Development. No-cost training at local criminal justice academies or police agencies is also advisable.

20-6
Operational Restrictions for Interns

a. CID interns are not authorized to carry any credentials that identify them as law enforcement personnel. Interns are not authorized to carry firearms or any other weapon. Interns will not be placed in a situation where it would be necessary for them to use force to subdue an individual or to be exposed to force themselves. The safety of interns is of foremost importance. Interns will not be placed in situations where they may be exposed to potentially violent situations, such as raids or violent offender apprehensions.

b. An intern’s function is to accompany the agent supervisor during the course of duties to observe the performance of non-violent CID duties. Interns should practice CID mission-essential tasks to gain hands-on experience. Interns will not collect evidence or be involved in the chain of custody in order to preclude the necessity for their testimony in court proceedings. Interns will not execute rights advisement, conduct criminal apprehensions, or suspect interviews. Interns may, however, witness the rights advisement and may assist during interviews of suspects, witnesses and victims that are conducted by CID agents. The swearing of persons to statements by interns is not authorized. Care should be taken not to involve the intern in activities where they may be called out of a future BSAC to testify at courts and boards. Interns may obtain non-significant statements and conduct non-significant witness interviews; however, the statements must be reviewed, approved for content and format, and sworn to by a CID agent. Interns may assist in the logistics of CID investigative duties, e.g., crime scene and photographic equipment set-up, fingerprinting and photographing suspects, etc. They will be instructed that, although they have access to a great deal of sensitive information, they have no authority to release any information. Each intern will be required to acknowledge in writing that they have read these restrictions and understand what their authorities and responsibilities are (Figure 20-2). This acknowledgement will be filed in their CID individual training record.

c. Use of force by CID interns.

(1) Although interns are not law enforcement personnel, they will become familiar with use of force policy by law enforcement personnel.

(2) Depending on the availability of training ammunition, interns should be trained and become familiar with the operation and maintenance of CID duty weapons.

d. An intern’s status will never be upgraded to criminal investigative assistant. In the event an intern is allowed to remain with the CID office pending attendance to the BSAC, their duties will remain with the same restrictions. They should continue to be closely supervised to ensure their safety, that investigations are not compromised, and that the rights of suspected/accused persons are protected.

20-7
Documentation of Training

a. The intern training progress will be recorded monthly on CID Form 120-E-R in the same manner as probationary agents. The reverse side of the form will be annotated with the investigations on which the intern assisted. The intern will be given constant feedback concerning his/her duty performance and counseled

monthly by the supervising agent. CID intern training records will be maintained in the same fashion as the training records of CID probationary agents.

b. After completion of three months internship, the SAC will recommend to the Accreditation Division whether the intern should be scheduled to attend the BSAC after projected completion of six months internship. The individual can then be given a tentative school date while completing the required six months internship.

c. The SAC will formally recommend approval or disapproval for CID acceptance in a memorandum addressed to the Commander, USACIDC, ATTN: CISP-AC (Figure 20-3). The recommendation will reflect that the applicant has satisfactorily completed at least 6 months of documented criminal investigative training with a CID unit and must include a final evaluation on a CID Form 120-E-R.

Figure 20-1. Application for CID Intern Training Program

APPLICATION FOR CID INTERN TRAINING PROGRAM

Office Symbol Date

MEMORANDUM FOR Commander, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506

SUBJECT: Application for CID Intern Training Program

1. Reference CID Regulation 195-1 (Criminal Investigation Operational Procedures), Chapter 20, USACIDC Intern Training Program.

2. In accordance with the above reference, request acceptance for CID training for SGT John/Jane B. Doe, 123-45-6789.

3. As reflected in the attached Application for Acceptance as a USACIDC Agent, SGT John/Jane B. Doe is fully qualified except for the required law enforcement experience.

4. SGT John/Jane B. Doe understands that the purpose for entering this training program is to gain a minimum of six months law enforcement training in order to obtain a waiver of the police experience prerequisite outlined in AR 195-3. Also, that acceptance for CID intern training does not constitute final acceptance for training as a CID special agent and that intern training may be terminated for substandard performance or behavior, or a demonstrated lack of aptitude or suitability for CID duties. SGT John/Jane B. Doe understands that he/she may terminate training and withdraw his/her CID application voluntarily; for any reason, without prejudice.

(signature block)
Special Agent-In-Charge

Encl
CID Application

Figure 20-1. Application for CID Intern Training Program

Figure 20-2. CID Intern Declaration of Understanding

CID INTERN DECLARATION OF UNDERSTANDING

1. My past record, both military and civilian, have been or will be examined and checks made to determine if I have had any problems, past or present, with police agencies.

2. I am not a CID agent and will not represent myself as such in any way, at any time, or under any circumstances. I will not apprehend or attempt to apprehend/arrest anyone.

3. I am not authorized to carry a weapon at any time, except for firearms during formal unit weapons training at a range. A weapon is a gun, knife, club, protective spray, or similar type of item.

4. I am not authorized to possess, use, or purchase illicit drugs, stolen property, illegal weapons, or other contraband.

5. I will have access to a great deal of sensitive information. I have absolutely no authority to release any information.

6. I will not knowingly violate any laws.

_____ _____
SIGNATURE OF INTERN DATE

_____ _____
SIGNATURE OF AGENT SUPERVISOR DATE

Figure 20-2. CID Intern Declaration of Understanding

Figure 20-3. Completion of CID Intern Training Program

COMPLETION OF CID INTERN TRAINING PROGRAM

DEPARTMENT OF THE ARMY
United States Army Criminal Investigation Command
Fort Blank Resident Agency, 4th Military Police Group (CID)
Fort Blank, GA 30050-5000

Office Symbol Date

MEMORANDUM FOR Commander, USACIDC, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506

SUBJECT: Completion of CID Intern Training Program

1. During the period _____, SGT John/Jane B. Doe, SSN # 123-45-6789, received CID intern training at this office. SGT Doe worked under the direct supervision of accredited CID special agent _____. His/her training was documented monthly on CID Apprentice Agent Monthly Evaluation reports on file at this office. SGT Doe satisfactorily completed his/her intern training period as documented on the attached terminal evaluation report.

2. I recommend/do not recommend SGT Doe be granted a waiver IAW AR 195-3, paragraph 2-2a(14) on the basis of CID intern training.

Encl (signature block)
CID Form 120-E-R Special Agent-In-Charge

Figure 20-3. Completion of CID Intern Training Program

CHAPTER 21

21-1
Purpose

This chapter prescribes policy and procedures for the release and processing of allegations of misconduct against all CID investigative personnel, to include laboratory examiners.

21-2
Policies

Allegations against military and civilian special agents and laboratory examiners will be processed IAW this chapter. Chapters 4 and 5 of this regulation will be used as a general guide. In the event commanders or directors are not certain whether a given allegation requires an investigation they should consult with their group legal advisor or the MACOM Labor Counselor.

21-3
Responsibilities

a. The CG, USACIDC, is the final authority regarding elimination of all special agents and laboratory examiners from the CID program.

b. DCSSPT, HQUSACIDC, is responsible for monitoring all allegations of special agent misconduct and related investigations and providing updates to the DCO. The DCSSPT is also responsible for aggregating and analyzing all reported special agent misconduct. The DCSSPT will publish periodic reports on special agent misconduct which highlight patterns and trends in special agent misconduct and offer guidance for their detection and prevention, and disseminate these reports throughout the command.

(1) The Accreditation Division, HQUSACIDC, is the proponent and lead staff agency for the management and headquarters coordination of all special agent and laboratory examiner misconduct actions and will monitor all special agent misconduct allegation actions. The Accreditation Division will:

(a) Receive initial notification of allegations of special agent misconduct and special agent suspensions from major subordinate command (MSC) commanders.

(b) Notify the Deputy Commander (DCO), Deputy Chief of Staff for Operations (DCSOPS), the Office of the Staff Judge Advocate (OSJA) and the

Crime Records Center (CRC) of the initiation of commander's inquiries and special agent suspensions.

(c) Provide monthly updates to the DCSSPT on the status of every special agent misconduct action.

(d) Manage the processing of military elimination actions within HQUSACIDC.

(2) The Civilian Personnel Division (CPD), DCSSPT is responsible for managing adverse personnel actions against civilian special agents.

c. USACIDC personnel are responsible for maintaining the standards in AR 195-3 for reporting known or suspected incidents of misconduct, both criminal and non-criminal, by USACIDC personnel.

21-4
Standards

a. No one has an inherent right to be a CID agent or laboratory examiner. At the discretion of the CG, USACIDC, any individual who is considered substandard in performance or conduct, deficient in character, or otherwise unsuited for the CID program will be not be accepted or retained.

b. Use of a CID agent’s or laboratory examiner’s conviction by court-martial or a civilian criminal court, or punishment under the provisions of Article 15, UCMJ, in support of elimination from the CID program under this regulation does not constitute double jeopardy.

c. CID agents and laboratory examiners are in positions of special trust and confidence. Therefore, CID agents and laboratory examiners may be eliminated from the CID program for any of the following reasons:

(1) Loss of credential, badge, any part thereof, or weapon through negligence.

(2) Purposely or through negligence failing to secure or account for evidence or contingency limitation (.0015) funds.

(3) Indiscretion, disaffection, breach of discipline, or abuse of privilege reflecting adversely on the USACIDC or the Army.

(4) In the case of military CID agents or laboratory examiners, any of the reasons that subject an individual to elimination from the Army under the provisions of AR 635-200 or AR 600-8-24.

(5) Any acts or omissions that could impair the ability to perform effectively any CID program duties such as loss of security clearance or failure to maintain qualifications to carry a weapon. This prohibition includes any violation of the UCMJ, the commission of a criminal offense or the criminal violation of foreign law.

(6) Moral or professional dereliction, acts of intemperance to the discredit of the service, or intentional omissions or misstatements of facts in official statements.

(7) Substandard duty performance.

(8) Failure to complete the prescribed apprentice or probationary period successfully.

(9) Failure to honor a mobility agreement.

(10) Any discharge of a weapon through negligence.

d. U.S. Army Reserve (USAR) and National Guard (NG) CID agents who fail to successfully complete the USAR Criminal Investigation Course or the CID Basic Special Agent Course within a 24-month period after initial acceptance may be eliminated from the CID Program.

21-5
Policy

All military CID agents may voluntarily request reassignment to other than criminal investigative duties. This would include, once approved, a reclassification to another MOS IAW the needs of the Army.

21-6
Procedure

Military CID agents requesting voluntary release from the CID program, must submit a written request stating the basis for the voluntary release. Justification to support the agent’s release from the program must be provided with endorsements through the chain of command. Requests for voluntary release will be forwarded to the HQUSACIDC, ATTN: CISP-AC, for processing and approval by the DCSSPT. Upon receipt of the approved release, the agent must submit a DA Form 4187 requesting voluntary reclassification IAW AR 614-200. The request must contain a copy of the approval endorsement from HQUSACIDC and turned into the Field Reclassification Authority (FRA) for PERSCOM

approval. A copy of the approved reclassification action must be provided to HQUSACIDC, ATTN: CISP-MP

21-7
Investigations

a. Preliminary Inquiry. Upon receipt of any information alleging misconduct, the supervisor of the CID agent or laboratory examiner will immediately notify the first field grade commander or, in the case of civilian CID agents or examiners, the first director, in the agent's chain of command. The commander or director will then immediately notify the rest of the chain of command through the group commander. The battalion/district/field office commander or the director will consult the supporting CID legal advisor and, in the case of civilian special agents or examiners, the USACIDC Labor Counselor and Chief, Civilian Personnel Division (CPD), HQUSACIDC. The battalion/district/field office commander or director will then conduct a preliminary inquiry to determine whether the allegation is credible. The preliminary inquiry will be completed within 5 working days.

(1) If the preliminary inquiry proves that the allegation is without merit, no further inquiry is required. A memorandum for record (MFR) will be prepared documenting the allegation and a summary of the commander's preliminary inquiry. The MFR and related inquiry documents will be forwarded through the appropriate group legal advisor and commander to HQUSACIDC, ATTN: CISP-AC, not later than 5 working days following completion of the preliminary inquiry. These documents will be reviewed for investigative sufficiency by the DCSOPS, for legal sufficiency by the OSJA and be filed in the Accreditation Division.

(2) If the preliminary inquiry establishes some substance to the allegation or fails to refute the allegation within the 5 working day period, a commander's inquiry will be initiated.

b. Commander's Inquiry. After coordinating with the group commander and group legal advisor, the battalion/district/field office commander or, in the case of civilian special agents or examiners the appropriate director, will initiate a commander's inquiry into allegations of special agent misconduct.

(1) The battalion/district/field office commander or director will appoint an investigating officer in writing (see example at Figure 21-1). The group commander will immediately notify HQUSACIDC, ATTN: CISP-AC upon initiation of a commander's inquiry. The commander's inquiry will be completed within 30 working days from the completion of the preliminary inquiry. Extension requests will be submitted through the chain of command to HQUSACIDC, ATTN: CISP-AC for the DCO's approval.

(2) Within 5 working days of the completion of the commander’s inquiry the battalion/district/field office commander or director will forward the completed commander's inquiry to the group commander with recommendations for action. The Directors, USACIL and USACRC, will forward their inquiries to HQUSACIDC, ATTN: CISP-AC for the DCO, USACIDC.

c. When either the preliminary inquiry or commander’s inquiry indicates a criminal offense has occurred (other than APCSM), a criminal investigation will be conducted IAW chapter 4 of this regulation (see paragraphs 4-7 and 4-8) and will be completed within 30 days. A USACIDC case number (sequence and ROI numbers are required) will be assigned to criminal allegations and subject(s) will be listed based on the credibility standard. All criminal investigations initiated pursuant to a preliminary or commander’s inquiry will be conducted as Category I investigations IAW paragraph 4-6b(1) of this regulation. Requests for extensions beyond 30 days for completion of a criminal investigation will be forwarded to this headquarters, ATTN: CISP-ZA for approval. A commander’s inquiry or preliminary inquiry will not be closed upon the initiation of an ROI. Typically, the ROI is made a part of a commander’s inquiry, and the inquiry addresses those issues or matters not covered by the ROI.

d. The investigating officer for preliminary inquiries will be a non-commissioned officer (95D), warrant officer (311A), commissioned officer (31A), a civilian special agent (1811), or a laboratory examiner and will be senior in rank to the person under investigation. The investigating officer will coordinate closely with the group legal advisor and, in cases of allegations against civilian CID agents or laboratory examiners, the USACIDC Labor Counselor, throughout the investigation. All relevant witnesses will be identified and interviewed.

e. A polygraph may be offered and conducted IAW this regulation. The refusal to take a polygraph will not be considered in any recommendation or decision regarding suspension or elimination from the CID Program. If a polygraph is administered, however, the results may be considered by the chain of command, and in the case of military special agents by the Accreditation Review Board (ARB) and by the CG.

21-8
Commander's action

a. Whatever action a group commander decides to take, a complete copy of the preliminary inquiry, commander’s inquiry and related documents will be forwarded to the HQUSACIDC, ATTN: CISP-AC. These documents will be reviewed for investigative sufficiency by the DCSOPS, for legal sufficiency by the OSJA and for filing by the Accreditation Division.

b. For civilian CID agents and laboratory examiners, the appropriate battalion/district/field office commander or director will take action described in c and d below.

c. When a preliminary inquiry or commander's inquiry (1) results in a criminal investigation, or (2) reveals that the allegation is founded and, in the judgment of the group commander, could support elimination from the CID Program, the commander will:

(1) Suspend the CID agent or examiner from all investigative duties and assign to administrative duties with a CID unit or temporarily detail the suspended CID agent to a non-CID unit for duty.

(2) Withdraw the CID agent's or examiner’s badge, credentials, official passport, pistol and ammunition.

(3) In the case of military CID agents, initiate a flagging action IAW AR 600-8-2.

(4) Suspend the CID agent's or examiner’s security clearance on an interim basis pursuant to AR 380-67.

(5) Immediately notify HQUSACIDC, ATTN: CISP-AC through the group commander.

(6) Complete the investigation unless notified that HQUSACIDC has assumed responsibility for the investigation.

d. Reinstatement from Suspension Pending Inquiry or Investigation:

(1) CID agents or examiners who are subjects in a founded ROI will remain suspended until the CG, USACIDC, reinstates them.

(2) In all other cases, unless relieved of the responsibility for the investigation, the group commander may reinstate the CID agent or examiner when the evidence indicates that the allegations will not result in the group commander recommending the special agent be eliminated from the CID program. The commander or director will immediately notify HQUSACIDC, ATTN: CISP-AC, of a reinstatement.

e. Civilian CID agents and laboratory examiners. The completed commander’s inquiry will be referred through the supervisory chain to the lowest independent supervisory level not connected with the incident. Normally this will be the first line supervisor of the special agent under investigation. That supervisor will coordinate with the USACIDC Labor Counselor and Civilian Personnel Division Chief before taking any action. All actions against civilian CID agents will comply

with the applicable civilian personnel regulations. The remaining provisions of this paragraph and paragraphs 21-7 though 21-13 do not apply to cases involving civilian CID agent misconduct.

f. Elimination and Retention:

(1) Within 5 working days of the completion of the commander's inquiry, the battalion/district/field office commander will forward the investigation together with recommendations for disposition to the group commander. Within 10 working days of the completion of a commander's inquiry, the group commander will decide whether a CID agent should be eliminated or retained and take the following action:

(a) If the decision is to retain and is within the group commander's authority (see subparagraph c. above), the commander will reinstate the CID agent.

(b) If the group commander decides that a CID agent who is a subject in a founded ROI should be retained, the commander will forward the investigation together with his recommendation to reinstate to the CG, USACIDC.

(c) If the group commander determines that a CID agent should be eliminated from the CID program, he will notify the CID agent in writing of his decision to recommend elimination (Figure 21-2) not later than 5 working days following his decision. The CID agent will be informed if he is entitled to appear before an Accreditation Review Board (ARB), provided with a copy of all documents pertaining to the recommendation to eliminate, advised that he may consult with the Trial Defense Service (TDS) or a civilian attorney at no expense to the government, and be given 10 working days to provide any matters in rebuttal (Figure 21-3).

(d) A CID agent entitled to an ARB may waive it conditioned upon being placed into a probationary status for one year. See paragraph 21-13c.

(2) Recommendations, investigative reports, allied documents/evidence to support the recommendation(s), as well as any matters submitted in rebuttal, will be forwarded through command channels to the Commander, USACIDC, ATTN: CISP-AC within 5 working days after the last involved action.

(3) An elimination action and Article 15 may be processed simultaneously. For example, a commander may give written notice of a recommendation to eliminate and offer an Article 15 at the same time. In this case, a CID agent's consultation with defense counsel can be comprehensive. If the circumstances warrant, a commander may recommend holding an elimination decision in abeyance until the completion of judicial or non-judicial actions.

(4) If the CID agent is eliminated from the CID program, the battalion/district/field office commander will provide a monthly status report on the soldier through the Group S-1 to HQUSACIDC ATTN: CISP-MP until the soldier is separated from the Army or reclassified and reassigned to a non-CID unit.

21-9
Action Concerning Commander's Recommendation

a. Upon receipt of the commander's recommendation and supporting documents, the Accreditation Division will forward the packet to the DCSOPS for an investigative sufficiency review and to the OSJA for a legal sufficiency review within 5 working days.

b. Following any corrective actions, the complete investigative report with recommendations will be forwarded to *[either:]*

(1) The CG, USACIDC, for final decision within 5 working days if the CID agent is not entitled to or has not requested an ARB; or

(2) An ARB if the CID agent is entitled to and has requested a board. The ARB will be appointed within 5 working days of the OSJA review.

21-10
Composition of the ARB

a. The purpose of the ARB is twofold:

(1) Give a CID agent the opportunity to explain why he or she should be retained in the CID Program; and

(2) Provide the CG with an independent assessment of whether a CID agent should be retained in the CID program.

b. All military CID agents are entitled to have their elimination from the CID program reviewed by an ARB except under the following circumstances:

(1) Conviction by any level of court-martial.

(2) Administrative elimination in lieu of a court-martial for enlisted personnel or resignation for the good of the service in lieu of general court-martial for officers.

(3) Receipt of an Article 15.

(4) Being an apprentice special agent or in a probationary status.

c. CID agents not entitled to an ARB may request the CG grant an exception. This request must be in writing and submitted with any documents provided in response to a notice of intent to recommend elimination pursuant to paragraph 21-6c(l)(c) of this regulation.

d. An ARB will review recommendations for elimination from the CID program together with all related evidence and rebuttals. The ARB will conduct its proceedings within 5 working days from appointment.

e. An ARB will consist of 5 members appointed by the DCSSPT, HQUSACIDC. The composition of the board will be as follows:

(1) For warrant officer CID agents - not less than 1 commissioned officer and 4 warrant officers, all with an equal vote.

(2) For enlisted CID agents - not less than 1 commissioned officer, 2 warrant officers, and 2 NCO members, all with an equal vote.

(3) For USAR or National Guard CID agents – at least one warrant officer or enlisted member, as appropriate, will be a member of the USAR or National Guard.

(4) All board members will be senior to the respondent CID agent.

(5) The commissioned officers will have military occupational specialty (MOS) 31.

(6) A non-voting recorder from the Accreditation Division or the OSJA to assist the president.

(7) The president of the board will be a field grade officer or higher.

(8) All noncommissioned officers (NCOs) and warrant officers selected for duty on an ARB will be accredited CID special agents.

f. If the ARB is reviewing a recommendation for elimination of a CID agent in a specialty program, i.e., polygraph, laboratory, etc., a member of the specialty program will be a voting member on the ARB when the allegation concerns abilities or functions of the specialty.

g. Board duty takes precedence over all other assigned duties.

21-11
Duties of the President of the ARB

The president of the ARB shall:

a. Set the date and location for the ARB. The ARB will meet at the call of the president.

b. Ensure that a summarized record is made of the board's proceedings.

c. Notify the respondent of the time and place that the board will convene and ensure that the respondent has copies of all documents the ARB will consider.

d. Ensure that arrangements are made for the respondent to appear before the board via video teleconference (VTC) or in person, if reasonably available.

21-12
Conduct of Proceedings

a. The president will call sessions to order and offer the respondent the opportunity to make a statement or present any evidence in the respondent's favor.

b. The respondent will represent him or herself. The respondent may consult with defense counsel, but counsel may not appear before the board.

c. The respondent may request witnesses to speak on his/her behalf. Names and locations of these witnesses will be provided in writing when the ARB is requested. The president will decide whether the witnesses are reasonably available to appear and whether substitutes for their live testimony, such as written sworn statements, videotaped statements or VTC appearances are appropriate.

21-13
Conclusion of ARB Proceedings

After reviewing all the evidence, the board will decide by secret written ballot whether to recommend retention or elimination from the CID program. The board may also recommend that the CID agent be returned to a probationary status for a period not to exceed one year. The board may make other recommendations it deems appropriate. A majority vote is required for any recommendation.

21-14
Report of Proceedings

a. The board report will include the summarized record and copies of all documents presented to and considered by the board. The board report will be signed by the board president within 5 working days of the conclusion of the board proceedings.

b. The final board report will be reviewed by the OSJA within 1 working day and submitted to the CG, USACIDC.

21-15
Final Action

a. If an ARB was held, the CG, USACIDC, may approve or disapprove the board's recommendations with or without modification.

b. If no ARB was held, the CG, USACIDC, will decide whether a CID agent should be placed on probation, retained or eliminated from the CID program.

c. The CG, USACIDC, may determine that a CID agent should be placed on probation for a period of time not to exceed one year. During the period of probation, the individual's conduct as a CID special agent will be closely monitored. The Accreditation Division will notify the USACIDC MSC concerning the decision and their responsibility to conduct quarterly evaluations of the special agent during the probationary period. Quarterly monitoring reports (Figure 21-4) will be forwarded to the Commander, USACIDC, ATTN: CISP-AC.

d. Quarterly Evaluation outcomes:

(1) After the one year probation period, the CID agent will return to accredited special agent status, unless performance, professionalism or other pertinent factors make it necessary to recommend elimination from the program.

(2) During the probationary period, a recommendation can be made at any time to discontinue the probationary status and eliminate the CID agent from the CID program if the CID agent demonstrates weaknesses warranting such a recommendation. The special agent will not be entitled to an ARB under such a circumstance.

e. The decision by the CG, USACIDC, is final and not subject to appeal.

f. The chief of the Accreditation Division will transmit decisions on elimination actions to the MSC commander within 3 working days of the CG’s decision.

21-16
Reclassification Process

a. Military CID special agents who are eliminated from the CID program based on misconduct must be processed for separation from the U.S. Army due to loss of MOS qualification. The following procedures apply:

(1) For warrant officers (MOS 311A), the following actions must immediately be initiated IAW Chapter 4-2, AR 600-8-24, Officer Transfers and Discharges:

(a) Local commander will FLAG officer IAW AR 600-8-2.

(b) Local commander will request initiation of elimination proceedings through the Group Commander to the General Officer Show Cause Authority (GOSCA) located in the geographic area of the officer concerned. An information copy of this action will be provided to this headquarters, ATTN: CISP-MP. The GOSCA will then notify the officer via memorandum that elimination action proceedings have been initiated and that they need to show cause for retention on active duty.

(c) Upon receipt of the officer's response (officer has 30 days to reply), the GOSCA must:

1. Close the case favorably, or:

2. If the officer desires to be discharged, resign, or retire in lieu of elimination proceedings, the appropriate paperwork will be forwarded to PERSCOM (officer will be separated NLT 30 days after receipt of approval for separation), or:

3. If the officer does not wish to be eliminated, the GOSCA will direct a Board of Inquiry to evaluate the officer (board must be completed NLT 90 days from the date the GOSCA directs the board). PERSCOM must be notified of the intent to conduct the board. Board of Inquiry results will be processed as outlined in AR 600-8-24, paragraph 4-6 and table 4-1.

(2) Enlisted special agents, MOS 95D, must be processed for separation under AR 635-200, Enlisted Personnel, to the local separation authority (special court-martial convening authority). The local separation authority will follow the guidelines established in AR 635-200 and will:

(a) Separate the soldier, or

(b) Decide to retain the soldier on active duty. A copy of the written decision to retain the soldier must accompany a request for mandatory reclassification to be processed through the local field reclassification authority (FRA) for

PERSCOM approval. A copy will also be forwarded to this headquarters, ATTN: CISP-MP.

b. When a CID Special Agent, MOS 95D, loses qualification in their MOS based solely on inefficiency or failure to complete the prescribed apprenticeship, a request for release from the CID program must be forwarded through the special agent's chain of commander. Requests must be forwarded to HQUSACIDC, ATTN: CISP-AC, for approval by the CG. Upon receipt of approval, the unit commander will process the special agent for mandatory reclassification. The request will be processed through the local FRA for PERSCOM approval. A copy will be forwarded to HQUSACIDC, ATTN: CISP-MP.

c. Reserve personnel who are released from the CID program based on misconduct will be processed for MOS reclassification through their unit of assignment for final action at ARPERSCOM or NGB, where applicable.

CHAPTER 22

22-1
Purpose

This chapter establishes procedures and provides guidance for the issue and control of badges, credentials, laboratory and polygraph certificates, and CID special agent sequence numbers.

22-2
Explanation of terms

a. Badge - A distinctive shield, issued in conjunction with the special agent, supervisor, laboratory examiner or staff credentials, as defined later in this chapter. The badge allows immediate identification and is normally associated with law enforcement/investigative operations.

b. Credential - An identification document issued to U.S. Army military and civilian personnel involved in CID related duties.

c. The CID generic credentials - An identification document issued to U.S. Army military and civilian personnel involved in CID related duties, but not accredited as special agents.

d. Indigenous personnel identification card - An identification document issued to foreign national investigators, interpreters, translators, and laboratory personnel performing duties in direct support of criminal investigations.

e. Polygraph examiner certificate - A numbered certificate issued to a special agent, which identifies an individual as a certified polygraph examiner.

f. Laboratory examiner certificate - A certificate issued to an individual, which identifies an individual as a certified laboratory examiner.

g. CID personnel sequence number - A four-digit number used by CID to identify CID special agents and others described in paragraph 22-14.

22-3
Objectives

To ensure the proper issuance and safeguarding of credentials, badges, indigenous identification cards, laboratory and polygraph certificates, and sequence numbers.

22-4
Responsibilities

a. The CG, USACIDC, is the final approving authority for the issuance of CID badges, credentials, identification cards and certificates described in this chapter. These items are the property of the U.S. Government and will not be altered. Therefore, the CG can withdraw them at any time. All CID badge and credential designs must be approved by the CG. Requests for the issue of badges and credentials must cite requirement/authorization from this chapter and/or include detailed justification when appropriate.

b. The Accreditation Branch is responsible for staffing credentials and certificates requiring the CG's approval/signature. The Accreditation Branch is also responsible for the issue, control and accountability of all badges and credentials for special agents, supervisors and staff.

c. Battalion commanders are responsible for the issuance of the indigenous personnel identification card (CID Form 63) to foreign national employees.

d. Battalion commanders are responsible for the issuance and accountability of the CID generic credentials to authorized personnel.

e. The USACIL commander is responsible for issuance and accountability of laboratory examiner badges. The examiner badge design must identify the examiner as a "Laboratory Examiner" on the face of the badge. The laboratory examiner badge will be issued after the CG approves the examiner's credentials.

22-5
Issue of CID agent badges and credentials

a. A numbered badge will be provided to each special agent with the special agent credentials. The credentials (DA Form 3638) are numbered and will include name, photograph, physical description, signature, and date of issue. All credentials are signed by the CG, USACIDC. The badge and credentials will be issued to:

(1) Active duty personnel upon successful completion of the Basic Special Agent Course (ASAC) at the U.S. Army Military Police School (USAMPS).

(2) Reserve Component personnel who have achieved accreditation.

(3) Civilian special agents after completing all conditions of employment and training requirements.

b. Special agent credentials require submission of two (untrimmed) color photographs of the individual, which when trimmed (at the Accreditation Branch) will be 1 1/2 inches by 1 7/8 inches of the head and shoulders. Both photographs will be taken of the individual in civilian clothes (male: coat and tie and female equivalent dress) without head cover. The photographs will be taken from a full front view with the subject looking directly into the camera. A title board, reflecting the name of the subject for identification of the photographs only, will appear outside the above-cited dimensions (figure 22-5). Single layer Polaroid type, or instant passport sized photographs are acceptable.

(1) Personal data pertaining to the individual will include:

(a) Height (indicated in inches, i.e., 70").

(b) Weight.

(c) Color of eyes.

(d) Color of hair.

(2) Hair and mustache lengths will conform to current military standards for military personnel.

(3) Active and Reserve Component personnel exceeding the screening table of AR 600-9 must submit a current DA Form 5500-R or DA Form 5501-R, where applicable.

22-6
Issue of the CID special agent oath

The special agent oath is administered and the certificate (CID Form 64) is presented upon graduation from the BSAC. The annotated, signed, and countersigned second copy of the oath (CID Form 64-1) will be returned to the Commander, USACIDC, ATTN: CISP-AC. The oath suffices as a receipt for the badge and credentials.

22-7
Issue of the supervisor badge and credentials

CID Forms 62 and 62-1 are issued to identify a CID supervisor.

a. The supervisor badge and credentials will be issued to the following duty positions:

(1) DCO, USACIDC.

(2) DCSOPS, USACIDC.

(3) Major subordinate commanders; battalion/district and field office commanders; USACIL Commander; and their executive officers.

(4) Deputy major subordinate commanders.

(5) USACIDC major subordinate command, battalion/district and USACIL commissioned operation officers.

b. Requests (figure 22-1) for supervisor badges and credentials must include:

(1) Two (untrimmed) color photographs of the individual, which when trimmed (by the Accreditation Branch) will be 1 1/2 inches by 1 7/8 inches of the head and shoulders. Both photographs will be taken of the military member in Class A uniform only, without head covering. Civilian personnel will wear appropriate business attire. The photographs will be taken from a full front view with the subject looking directly into the camera. A title board, reflecting the name of the subject for identification of the photographs only, will appear outside the above-cited dimensions. (See figure 22-5.) Single layer Polaroid type or instant passport sized photographs are acceptable.

(2) Personal data pertaining to the applicant, including:

(a) Height (indicated in inches, i.e., 70").

(b) Weight.

(c) Color of eyes.

(d) Color of hair.

(3) A statement from the applicant's commander stating the duty position the applicant is filling.

(4) Active and Reserve Component personnel exceeding the screening table of AR 600-9 must submit a current DA Form 5500-R and DA Form 5501-R, where applicable.

22-8
Issue of the laboratory examiner badge and credentials

The laboratory examiner badge and credentials (CID Form 62 and 62-1), will be issued to civilian laboratory examiners assigned to and/or employed by USACIL. All credentials are annotated to reflect the forensic field of employment of the holder (i.e., chemist, questioned document examiner, latent print examiner, firearms examiner, photographer) Requests (figure 22-2) will include:

a. Data required by paragraph 22-7b (1 through 4) above, as appropriate.

b. Statement by the laboratory commander that the individual has completed training or has satisfactorily demonstrated the ability to perform independent forensic analysis in their specific discipline.

22-9
Issue of the indigenous personnel identification card

The Indigenous Personnel Identification Card (CID Form 63) is numbered and printed in English and the language of the host country. It will include the individual's name, photograph, signature, date of issue, type of duty performed, and signature of the authenticating USACIDC major subordinate commander or USACIL commander. The USACIDC major subordinate commander and USACIL commander provides the CID Form 63. It is issued to foreign national investigator/interpreter and translator personnel requiring identification in the performance of official duties. Prior to issuance of CID Form 63, a thorough background check will be conducted in accordance with local procedures established by the major subordinate commander. A copy of this check will be maintained in the files of the issuing headquarters.

22-10
Issue of the laboratory examiner certificates

a. The Laboratory Examiner Certificate (CID Form 116) will include the individual's name, forensic discipline, and date authenticated by the CG, USACIDC.

b. The Laboratory Examiner Certificate (CID Form 116) is issued to military and U.S. civilian forensic examiners who have successfully completed the USACIL Program of Instruction (POI) in their discipline or who have demonstrated their proficiency as an examiner during their probationary hiring period.

c. Requests for issuance of the Laboratory Examiner Certificate will be forwarded through command channels upon the recommendation of the

laboratory commander. The Commander, USACIL will recommend approval or disapproval and indicate reasons for disapproval, if applicable.

d. Retention of certification is dependent upon the examiner's continued proficiency based upon regular conduct of forensic examinations. In the event an examiner is assigned to duties outside the laboratory for a period in excess of one year, their certification will be suspended until he/she has completed refresher training.

e. Certification as a laboratory examiner is effective until withdrawn by the CG, USACIDC.

22-11
Issue of the polygraph certificate

a. The Polygraph Examiner Certificate (DA Form 3833) is numbered and will include the individual's name and date issued. The certificate is authenticated by the CG, USACIDC. It is issued to applicants who have successfully completed the Polygraph Examiner Training Course and a minimum of six months internship under a certified examiner, during which they demonstrate proficiency as an examiner. The Director, USACRC, will make recommendations for issuance.

b. Applications (figure 22-3) forwarded through command channels will contain documentation of completion of the Polygraph Examiner Training Course. Intermediate commanders will recommend approval or disapproval and include reasons for disapproval, if applicable. Upon approval by CG, USACIDC, a certificate will be issued to identify the individual as a certified polygraph examiner.

c. Retention of certification is dependent on the examiner's continued proficiency based on regular conduct of polygraph examinations.

d. Certification as a polygraph examiner is effective until withdrawn by the CG, USACIDC.

22-12
Issue of the CID staff badge and credentials

The CID staff badge and credentials (CID Forms 62 and 62-1) may be issued to non-accredited military and civilian criminal intelligence coordinators/ investigators, and USACIDC staff personnel who are required to make frequent contact and coordination with allied and civilian police agencies or to conduct inquiries in support of the criminal investigative mission. The individual is not

entitled to the rights of the accreditation review procedures and it does not allow him/her to act in the capacity of an accredited criminal investigator.

a. Issuance of the staff badge and credentials will only be considered based on the recommendations of the supervisory chain of command. Therefore, any requests for issue must contain complete justification.

b. Staff badges and credentials will only be issued to those personnel who have a current, favorable single scope background investigation (SSBI). The possession of the credentials must benefit the individual in the performance of their duties. Applications (figure 22-4) will include:

(1) Two untrimmed color photographs of the individual, which when trimmed (by the Accreditation Branch) will be 1 1/2 inches by 1 7/8 inches of the head and shoulders. Both photographs will be taken of the individual in appropriate attire as indicated below:

(a) Military personnel must wear the class A uniform

(b) Male civilian personnel must wear coat and tie and female civilian personnel must wear appropriate equivalent attire.

(2) The photograph will be taken from a full front view with the subject looking directly into the camera. A title board, reflecting the name of the subject for identification of the photograph only, will appear outside the above-cited dimensions. See figure 22-5. Single layer Polaroid type or instant passport sized photographs are acceptable.

(3) Personal data pertaining to the individual will include:

(a) Height (indicated in inches, i.e., 70").

(b) Weight.

(c) Color of eyes.

(d) Color of hair.

(4) Active and Reserve Component personnel exceeding the screening table of AR 600-9 must submit a current DA Form 5500-R and 5501-R, where applicable.

22-13
Issue of the CID generic credentials

a. The CID generic credentials (CID Forms 62-2 and 62-3) may be issued as a form of identification to the following non-special agent personnel:

(1) Investigative Operations Assistants (IOA).

(2) Drug Suppression Team (DST) members.

(3) Military Police (MP) who are assigned/attached to a CID field investigative element under the direct supervision of a CID special agent and/or supervisor, and who perform investigative functions for CID.

(4) Military Police investigators (MPI),not in receipt of MPI credentials, who are assigned/attached to a CID field investigative element under the direct supervision of a CID special agent and/or supervisor, and who perform investigative functions for CID.

b. The CID generic credentials will not be issued to the following individuals:

(1) Personnel who are considered attached as on-the-job training (OJT) personnel.

(2) MP/MPI personnel attached/assigned to CID, if MP/MPI badges/credentials have been issued by the appropriate provost marshal for DST and/or investigative purposes.

c. The CID battalion/district commander is designated as the issuing authority for the generic CID credentials. The battalion/district commander will not delegate this authority. Each CID battalion/district will develop a program for the control, inventory, safeguarding, issue, and turn-in of the generic credentials. At a minimum, the battalion/district commander will require subordinate elements to inventory generic credentials and report the results of such inventory to the district office during August and February annually. At a minimum, the following will be accomplished for each credential holder:

(1) A CRC name check and a local military and police records check.

(2) For DST/MP/MPI personnel, a statement of agreement between the credential holder, credential holder's unit commander and the supervising special agent-in-charge regarding terms and standards of work with CID, training, length of assignment, methods of withdrawal of credentials due to misconduct or poor performance, attendance at unit formations, etc., will be executed prior to assignment/attachment and issue of the generic CID credentials. A similar statement may be generated for the investigative operations assistants, if

deemed appropriate. A combined Memorandum of Understanding (MOU) is sufficient for the statement of agreement requirement.

d. Generic credentials require submission of the following items to the district commander:

(1) A completed interview worksheet, containing the personal data pertaining to the applicant including:

(a) Height (indicated in inches, i.e., 70").

(b) Weight.

(c) Color of eyes.

(d) Color of hair.

(2) Two sets of applicant fingerprint cards.

(3) Two color photographs of the individual, 1 1/2 inches by 1 7/8 inches of the head and shoulders. Both photographs will be taken of the individual in civilian clothes (male must wear coat and tie and equivalent dress for female) without head cover. The photographs will be taken from a full front view with the subject looking directly into the camera. A title board, reflecting the name of the subject for identification of the photographs only, will appear outside the above-cited dimensions (figure 22-5). Single layer Polaroid type or instant passport sized photographs are acceptable.

e. The interview worksheet, statement of agreement or MOU, results of name checks, remaining photograph and both fingerprint cards will be placed in a folder and retained by the district office. The retention period of the folder, following the departure of the holder from the control of the issuing battalion/district, will be in accordance with the provisions of the Modern Army Record Keeping System (MARKS).

f. The bottom portion of the credential will bear the credential holder's photograph, signature and other personal data. The area below "authorized by" will bear the typed name of the issuing battalion/district commander and battalion/district office. The battalion/district commander will sign above the printed "battalion/district commander" signature block line.

g. The CID battalion/district office will develop a database or ledger system bearing the control number of the credential, date of issue and to whom issued for control purposes. Additionally, a security safeguard will be implemented to validate the holder of the credential, over time. For example, a termination date

appended to the top and bottom portions of the credentials or requiring the credentials to be reissued upon change of the issuing authority.

h. The credentials, after being signed by the credential holder and CID battalion/district commander will be laminated, placed in the credential case and issued to the holder.

i. A CID badge will not be issued with the generic credentials, nor will any statement be added authorizing the credential holder to carry a weapon. MP/MPI/DST personnel may be authorized to carry weapons by use of DA Form 2818, if approved by the battalion/district commander and/or the provost marshal.

j. Generic credentials will not be reproduced for any purpose by subordinate units. HQUSACIDC, CISP-AC (Accreditation Branch) is the proponent for the credentials. Should the need arise for additional credentials, coordination will be conducted with the HQUSACIDC distribution center for re-issue. DA Form 17 will be used to request the forms needed.

22-14
Issue of CID personnel sequence number

a. The CID sequence numbers are issued to:

(1) Active duty personnel upon successful completion of the ASAC (in residence) at the USAMPS.

(2) Reserve Component special agents upon accreditation and determination that the individual concerned will perform criminal investigative duties.

(3) Civilian special agents upon acceptance into the program.

(4) Civilian and military support personnel having a valid requirement for access to crime records.

(a) Requests for support sequence numbers will be forwarded to the Accreditation Branch for action. Requests will contain the individual's full name, SSN, grade, date of birth, place of birth, position, date SSBI completed, date clearance was granted, and justification for access.

(b) Access will be terminated when an individual vacates the position for which the sequence number was issued

(c) Sequence numbers will not be passed from incumbent to replacement.

(5) USACIDC personnel conducting telephonic criminal intelligence checks may be required to use the sequence number and/or badge number for security verification. Therefore, the numbers must not be openly displayed on calling cards, military coins and/or similar items that might compromise security. All are reminded not to provide their sequence number to other personnel for the purpose of conducting criminal history records checks. The USACRC maintains an audit trail on all released information, and who requested the information.

22-15
Controls

a. The badges, credentials, and laboratory examiner certificates are issued to the individual concerned by the Chief, Accreditation Branch. Polygraph certificates are issued by the Director, CRC.

b. Each individual is responsible for safeguarding their badge, credentials and/or polygraph certificate.

(1) Individuals who carry their badge and credentials will ensure they are under their immediate physical control or reasonably secured in their lodging.

(2) Reasonable security at a lodging means the badge and credentials are secured in such a manner so that its presence is not readily apparent and it is not easily accessible to unauthorized persons.

(3) Under only the most exceptional and unusual circumstances will CID investigative personnel temporarily store (not to exceed one hour) their badge and credentials in a privately owned or government owned vehicle. Under these circumstances, the badge and credentials will be stored in a locked glove box or trunk. Overnight storage in a vehicle is prohibited.

(4) CID investigative personnel will not surrender their badge and credentials to anyone unless as outlined in paragraph c (1) through (5) below.

c. CID investigative personnel responsible for carrying badge, credentials and/or polygraph certificate will surrender to, and obtain a receipt from the unit commander, operations officer, first sergeant or lawful authority under any of the following conditions:

(1) When suspension action has been initiated.

(2) When relieved of criminal investigative, supervisory, laboratory, or polygraph duties. This may occur as a result of withdrawal action in accordance with prescribed regulations, award of primary Military Occupational Specialty (MOS) outside of the criminal investigation field, permanent change of station

assignment to non-agent duties outside USACIDC, or upon retirement or release from active duty.

(3) When attending professional development training sites (warrant officer entry course, basic noncommissioned officer course (BNCOC), etc.). If TDY is scheduled en route, the item should be transferred to the gaining unit via registered mail.

(4) When required or ordered by a lawful authority (such as when visiting confinement facilities).

(5) When agents are assigned to branch immaterial positions.

d. Under the circumstances in b(1), (2), and (3) above, the unit commander will safeguard the badge, credentials and/or polygraph certificate, and return them to the individual only if that individual is returned to criminal investigative duties.

e. Whenever a special agent is permanently relieved from criminal investigative duties, the unit commander will seal the badge, credentials, and/or polygraph/laboratory certificate, and a copy of the orders (reclassification, retirement, ETS, etc.) in a double envelope and forward them by registered mail to the Commander, USACIDC, ATTN: CISP-AC.

f. When a civilian employee no longer requires a badge, credentials and/or polygraph/laboratory certificate for the performance of assigned duties, the badge, credentials and/or certificate will be surrendered and handled in the manner prescribed for military personnel in paragraph e above.

g. All USACIDC active duty commanders and U.S. Army Reserve and National Guard commanders of USACIDC units will maintain a record of all credentials, badges, and polygraph certificates held by criminal investigation personnel of their units. In addition, commanders will conduct a semiannual inventory of badges and credentials during the months of February and August. The roster reflecting the February inventory will be prepared and forwarded through the major subordinate command to the Commander, USACIDC, ATTN: CISP-AC, by 28 February on an annual basis. The roster will include the following minimum information: name, social security number; badge number; and credential number. In addition to this information, official passport information will be reported covering: type; date issued; location issued; date of expiration and passport number.

h. All major subordinate command and USACIL commanders of USACIDC units will maintain a master record of indigenous personnel identification cards issued by their office.

i. The Accreditation Branch will maintain a master record of all badges, credentials, sequence numbers, and official passport information issued by the USACIDC.

22-16
Loss, damage, or retirement

a. Loss.

(1) An individual will immediately report to their commander/supervisor the loss of any portion of their badge, credentials, or polygraph/laboratory certificate.

(2) The commander receiving the report will:

(a) Forward, by electronic mail, the notice of loss and identifying data to the Commander, USACIDC, ATTN: CISP-AC, with an information copy of the loss report furnished to the appropriate USACIDC major subordinate command/USACIL commander, if applicable. The HQUSACIDC will notify other major commands as appropriate.

(b) Commanders will follow appropriate procedures to initiate a preliminary inquiry to determine the facts relevant to the loss. Report facts, findings, action taken, and recommendations concerning the retention or withdrawal of accreditation in writing to the Commander, USACIDC, ATTN: CISP-AC. Comply with chapter 19 of this regulation when the commander recommends withdrawal of acceptance/accreditation.

(c) Upon notice of recovery of a lost badge, credentials, or polygraph/laboratory certificate, HQUSACIDC will transmit notification to all agencies previously notified of the loss.

b. Damage. Individuals will report to their immediate commander any damage to their respective badge and/or credentials. The individual's immediate commander will then submit a request for replacement of the credentials, badge, and/or polygraph/laboratory certificate, and a report of the circumstances of the damage through the USACIDC major subordinate command/USACIL headquarters to Commander, USACIDC, ATTN: CISP-AC. The damaged badge, credentials, and/or polygraph certificate will accompany the report via registered mail.

c. Retirement. All special agent personnel, CID supervisors, and staff members will return their badge, credentials, and holder, along with one copy of their retirement orders or personnel action, to Commander, USACIDC, ATTN: CISP-AC, using registered mail. The badge will be declared an item of gratuitous issue upon retirement after having served honorably. The credentials will be perforated with the word "RETIRED." A CID retirement plaque is available for purchase with funds normally provided by the individual concerned or a voluntary contribution of

funds from the subordinate field element. The cost of the plaque will be established through the Accreditation Branch in coordination with the appropriate vendor. If a retirement plaque is requested, a personal check or money order must accompany it for the predetermined amount, which includes shipping costs. The retirement plaque will reflect only the dates of CID service from acceptance into the CID program until retirement. This award will not be retroactive, as voided credentials are not retained in the Accreditation Branch indefinitely. Field elements are not authorized to design or prepare plaques of this type. Should the individual elect not to receive the plaque, the CID Form 42-1 with credentials only will be provided. If requested, the CID Form 93 (CID Special Agent Certificate of Service) is also available.

d. A memorial plaque is authorized for a CID agent who dies in the line of duty, without regard to age or length of service. A representative of the USACIDC major subordinate commander or battalion/district commander must notify the next of kin of the availability of the plaque. The plaque is identical to the retirement plaque, with the exception of the inscription and perforation on the credentials. The inscription plate reads "Presented to the Family of _____, in Memory of his (her) Loyal and Devoted Service to the U.S. Army Criminal Investigation Command, inclusive date".

e. Credentials of CID special agents who ETS from the service, or supervisors who PCS to assignments outside CID, are voided and affixed to the CID presentation certificate, CID Form 42-1. The certificate will be signed by the CG, USACIDC, and returned to the agent or supervisor provided their character of service was honorable and their accreditation status was intact. Departure from the service for failure to comply with the provisions of AR 600-9 and/or inefficiency in the performance of duties, resulting in non-selection for promotion, or bars to reenlistment negate presentation of the voided agent or supervisor credentials. Their badge is returned to the inventory for reissue and their sequence number invalidated. In that some special agents intend to enlist in a U.S. Army Reserve or National Guard CID unit after leaving the Regular Army, it is imperative that the Accreditation Branch be so advised of the individual's intent upon return of the badge and credentials. In all cases, the returned badge and credentials must be accompanied by action orders.

22-17
Badge and credential holders

The badge and credentials holder is provided with the initial issue of the badge and credentials.

a. The badge and credentials holder is normally replaced at U.S. Government expense when it becomes unserviceable through fair wear and tear. Determination of unserviceability and fair wear and tear will be made at the field

element level. Replacement of the holder will not be made unless the individual circumstances of the agent's service clearly indicate that the holder became unserviceable through no fault of their own. Holders that become unserviceable due to excessive abuse will be replaced at the agent's expense.

b. Requests for replacement of unserviceable holders will be made in writing to the Accreditation Branch.

22-18
Use and Display of CID Badge and Credentials

a. The special agent badge will not be unnecessarily displayed.

b. When identification is a requirement at a crime scene, the badge will be displayed.

c. When the agent’s weapon is carried exposed during a non-training event, the badge will also be displayed.

Figure 22-1. Request for Issue of Supervisor Badge and Credentials

LETTERHEAD

OFFICE SYMBOL (MARKS Number)

MEMORANDUM THRU Commander, XXXXX Group, …

FOR Commander, U.S. Army Criminal Investigation Command, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506

SUBJECT: Request for Issue of Supervisor Credential and Badge

1. In accordance with the provisions of USACIDC regulations, request that I be issued a supervisor badge and credentials.

2. On , I was assigned duties as the , and I meet the prerequisites of AR _____.

3. My personal data is as follows:

a. Height.

b. Weight.

c. Color of eyes.

d. Color of hair.

e. Security clearance verification.

f. Civilian education level.

Encl
Color Photos

SIGNATURE BLOCK

Figure 22-1. Request for Issue of Supervisor Badge and Credentials

Figure 22-2. Request for Laboratory Badge and Credentials

LETTERHEAD

Office Symbol

MEMORANDUM THRU Commander, USACIL

FOR Commander, U.S. Army Criminal Investigation Command, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506

SUBJECT: Request for Issue of Laboratory Examiner Badge and Credentials

1. In accordance with CID Regulation 19501, paragraph 22-8, request that I be issued laboratory examiner badge and credentials.

2. On _____, I was assigned to laboratory duties as._____.

3. My personal data is as follows:

a. Height.

b. Weight.

c. Color of eyes.

d. Color of hair.

e. Security clearance verification.

Encl
Color Photos

SIGNATURE BLOCK

Figure 22-2. Request for Laboratory Badge and Credentials

Figure 22-3. Request for Polygraph Certification

LETTERHEAD

OFFICE SYMBOL (Marks Number)

MEMORANDUM THRU

Commander, (subordinate field element)

Commander, (USACIDC major subordinate command)

FOR Director, U.S. Army Crime Records Center ATTN: CICR-PD, 6010 6th Street, Fort Belvoir, VA 22060-5506

SUBJECT: Request for Certification as a Polygraph Examiner

1. In accordance with AR 195-6, paragraph 3-2c, request that I be certified as a polygraph examiner.

2. The prerequisites outlined in AR 195-6, paragraphs 3-2c through 3-2e, have been complied with as indicated below:

a. I satisfactorily completed Polygraph Examiner Training Course (7H-711), Class number _____,on _____.

b. I completed a _____ month internship preceding submission of this application during which I conducted _____examinations.

(1) CW2 L. M. Kracklekorn, certificate # , Fort Bragg District, 3D MP Group (CID) .

(2) CW3 Michael Modern, certificate # , Fort Benning District, 3D MP Group (CID).

Encl
Copy of course diploma

SIGNATURE BLOCK

Figure 22-3. Request for Polygraph Certification

Figure 22-4. Request for CID Staff Credentials

LETTERHEAD

OFFICE SYMBOL (Marks Number)

MEMORANDUM FOR Commander, U.S. Army Criminal Investigation Command, ATTN: CISP-AC, 6010 6th Street, Fort Belvoir, VA 22060-5506

SUBJECT: Request for CID Staff Badge and Credentials

1. In accordance with CID Regulation 195-1, paragraph 22-12, request that Mr. William T. Doe be issued CID staff credentials.

2. On (Date), Mr. Doe was assigned to the duty position of criminal intelligence coordinator/investigator at the Fort Hood District CID office. (List complete justification.)

2 Encls
Photos

SIGNATURE BLOCK

Figure 22-4. Request for CID Staff Credentials

Figure 22-5. Sample Credential Photos

CHAPTER 23

23-1
Scope

The USACIDC Criminalistics Program pertains to the functional specialties of technical services and Field Investigative Equipment (FIE) acquisition.

23-2
Program objective

The objective of the Criminalistics Program is to optimize the criminal investigative posture of USACIDC by providing USACIDC investigators with state of the art investigative equipment, as well as operational support when requirements are beyond their capabilities.

23-3
Responsibilities

a. HQUSACIDC

(1) The Deputy Chief of Staff for Operations:

(a) Establishes policy and provides oversight to the USACIDC Criminalistics Program.

(b) Approves adoption of new techniques.

(c) Oversees the evaluation and acquisition of investigative equipment IAW CIDR 70-1, Evaluation and Acquisition of USACIDC Equipment.

(d) Oversees criminalistics training programs and sets minimum training standards for technical services coordinators, as well as training required to implement new equipment.

(2) The Deputy Chief of Staff for Support:

(a) Provides guidance concerning the acquisition of investigative equipment and serves as proponent for CIDR 70-1.

(b) Assures properly trained personnel are assigned to USACIL technical services.

(c) Provides a representative to the USACIDC Criminalistics Committee.

(d) Comptroller ensures that a level of funding commensurate with HQDA Program Budget Guidance (PBG) has been identified in the Command Budget Estimate (CBE) and the MACOM Program Objective Memorandum (POM) and is allocated during the fiscal year of execution to support the command criminalistics program.

(e) Makes recommendations for policy changes as needed.

(3) The USACIDC Assistant DCSOPS (ADCSOPS:

(a) Serves as the primary HQUSACIDC action officer for criminalistics matters.

(b) Chairs the USACIDC Criminalistics Committee.

(4) The USACIDC Criminalistics Committee:

(a) Defines USACIDC requirements for investigative equipment.

(b) Identifies investigative equipment to be evaluated by USACIL.

(c) Surfaces forensic science and technical services issues which need to be staffed and directs requirements to the appropriate HQUSACIDC staff office.

(5) The HQUSACIDC Forensic Science Officers:

(a) Advise the DCSOPS in matters pertaining to the development and use of FIE.

(b) Sit on the USACIDC Criminalistics Committee.

(c) Make recommendations for policy changes as needed.

(6) The US Army Military Police School (USAMPS) Chief of Physical Evidence represents USAMPS on the USACIDC criminalistics committee.

b. USACIL

(1) The Director:

(a) Assures the USACIDC Criminalistics Program, including the evaluation and acquisition of investigative equipment IAW CIDR 70-1, is managed to meet program objectives in a cost effective, efficient manner.

(b) Ensures the preparation of Operation and Maintenance, Army (OMA) and Other Procurement, Army (OPA) (e.g., Base- Level Commercial Equipment for

OPA-3, counter-terrorism and automation/communications equipment for OPA-2) budget estimates and plans to support acquisition of law enforcement and forensic science equipment.

(c) Oversees the fielding, maintenance, and disposition of forensic science and law enforcement equipment.

(d) Supervises the technical aspects of USACIDC's technical services program to include reviewing the use of technical surveillance and law enforcement equipment and techniques to assure it is consistent with investigative requirements.

(e) Manages technical services program assets to include making recommendations for the training and assignment of technical services coordinators and others with technical services responsibilities.

(f) Monitors policy associated with the application of technical services techniques and equipment as well as law enforcement equipment to assure it is consistent with investigative, administrative, and legal requirements.

(g) Make recommendations for policy changes as needed.

(2) The USACIL Forensic Science Officer:

(a) Sits on the USACIDC Criminalistics Committee.

(b) Conducts liaison with investigative, legal, scientific and medical professionals, as well as vendors of investigative equipment and supplies.

(c) Makes recommendations for policy changes as needed.

(3) The USACIL Technical Services Coordinator:

(a) Provides referrals to sources of training for technical services coordinators and agents in the field.

(b) Sits on the USACIDC Criminalistics Committee.

(c) Stays current in the technical services through review of professional literature, self-study, and continuing education to include attendance at professional meetings such as the annual meeting of the National Technical Investigators Association (NATIA).

(d) Make recommendations for policy changes as needed.

c. USACIDC Field Elements:

(1) All USACIDC commanders:

(a) Manage organic technical services assets to assure USACIDC realizes the full potential of their expertise and the Army maximizes the return on the investments made to train these personnel. This includes assuring the FSO and USACIL Technical Services Officer are consulted in investigations where their expertise would be helpful in resolving the matter under investigation and assuring effective use of unit coordinators in training of personnel under their command.

(b) Ensure investigative equipment and techniques, as well as training needed to support mission requirements, are identified IAW CIDR 70-1, CIDR 351-1 and this regulation.

(c) Promote the use of applicable forensic science and technical services techniques in the conduct of investigations under their control.

(d) Provide resources necessary to support training of forensic science and technical services coordinators as well as others assigned technical services responsibilities.

(2) Field Forensic Science Officers and Senior NCOs will:

(a) Provide consultation on investigations, advice to field agents, on site assistance, and training or briefings to assure state-of-the-art FIE is used in the conduct of USACIDC investigations within their respective areas of expertise and geographic areas of responsibility.

(b) Assist in the identification and evaluation of FIE and techniques as needed.

(c) Assure investigative equipment and technique needs are identified to the USACIDC major subordinate commander.

(d) Advise their commanders in all matters pertaining to the application of technical services techniques and investigative equipment.

(e) Assist subordinate units in the conduct of electronic surveillance training and briefings, and maintenance needed to support use of investigative equipment.

(f) Ensure field investigative equipment is in proper working order, overseeing the unit’s acquisition, storage, use, maintenance and disposition of the equipment.

(g) Make recommendations for policy changes as needed.

d. Armed Forces Institute of Pathology (AFIP) FSO.

(1) Makes recommendations for policy changes as needed.

(2) Sit on the USACIDC Criminalistics Committee.

23-4
General

The USACIDC will maintain a state of the art criminalistics capability and assure applicable technical services equipment is used in the conduct of USACIDC investigations.

23-5
Personnel and training

Personnel assigned to duties as technical services officers, as well as others assigned technical services responsibilities, will receive training consistent with their assigned responsibilities.

23-6
Equipment approvals

A guide on the use of investigative techniques and equipment, to include required approvals, is at Figure 23-1.

23-7
Funding

On site operational and training support provided by USACIL, other than training scheduled on an annual basis, will be funded by the USACIDC unit requesting the training.

23-8
USACIDC criminalistics committee

This committee will define USACIDC requirements for FIE. It will consist of the HQUSACIDC ADCSOPS, the HQUSACIDC, USACIL, and field FSOs; the

USACIL technical services officer; the AFIP FSO; the USAMPS Chief of Physical Evidence; DCSOPS Senior NCO; 701st Military Police Group (CID) Command Sergeant Major; and a representative from the HQUSACIDC Logistics Division. The committee will meet at least once a year, normally in conjunction with the annual meeting of the American Academy of Forensic Sciences.

23-9
General

Requests for operational support, training, existing equipment, and maintenance will be forwarded through the chain of command so they can be addressed at the lowest level with the resources and expertise to support the requirement. DoD forensic experts will be used to the greatest extent possible and needed support will be secured in the most cost effective manner possible.

23-10
Operational and training support

If the USACIDC MSC determines that needed training or operational laboratory, forensic sciences or technical services support is beyond the capabilities of the resources under his command, he should request support from the USACIL. Prior coordination between the USACIDC MSC coordinators and the USACIL Technical Support Division staff is encouraged to expedite services and identify the most efficient way to meet the needs. The USACIL will either provide on-site assistance or make appropriate referrals to meet the needs in an efficient, cost effective manner.

23-11
Equipment acquisition and maintenance

New equipment acquisition and maintenance requirements will be processed IAW applicable provisions of CIDRs 70-1 and 710-5 (Material Management System), as well as CID Pam 710-1 (USACIDC Catalog of Investigative Equipment.

23-12
Development of new investigative equipment

Requirements for new investigative equipment will be addressed through the USACIDC Criminalistics Committee. Immediate requirements should be

identified through the HQ FSO to the USACIL Technical Support Division by the USACIDC MSC.

Figure 23-1. Use Guide

Investigative Equipment and Techniques Use Guide

If the use is	And the application takes place	And the target is	Then final approval is required by	Emergency approval may be granted by	Guidance found in the following publications
Consensual Intercept of Oral or Wire Communication	Anywhere	Any person	Thru CID SJA to US Army General Counsel	Same	AR 190-53 and USACIDC Supplement 1
Nonconsensual Intercept of Oral or Wire Communication	CONUS	Any person	Thru CID SJA to US Attorney General	Same	AR 190-53 and USACIDC Supplement 1
	OCONUS	Any person	Thru CID SJA to US Army and DoD General Counsel	Same	18 US Code Section 2510 et. seq.
Dial Number Recorder (Pen Register)	CONUS	Any person	Thru CID SJA to US Army General Counsel **	Same	AR 190-53 and USACIDC Supplement 1
	OCONUS	Any person	Thru CID SJA to US Army or DoD General Counsel *	Same	18 US Code Section 3121 et. seq.
Line Trap and Trace Activity	CONUS	Any person	Post Commander or CDR, USACIDC **	Same	AR 190-53 and USACIDC Supplement 1
	OCONUS	Any person	Thru local SJA to Post Commander or CDR, USACIDC **	Same	18 US Code Section 3121 et. seq.

Optical Surveillance (Close Circuit TV or Photographic)	Anywhere	Any person or place	Battalion or Field Office Commander (Note 1)	Same
Signal Surveillance (when attached to the property of a consenting person)	Anywhere	Any person or place	Battalion or Field Office Commander	Same

Note: Refer to CIDP 710-1 for Catalog of Investigative Equipment

If the use is	And the application takes place	And the target is	Then final approval is required by	Emergency approval may be granted by	Guidance found in the following publications
Signal Surveillance (When attached to the property of a Non-consenting person i.e., tracking devices)	Anywhere	Any Person of place	Expectation of Privacy: Coordinate thru local SJA *	As delegated by CDR, USACIDC *	
			No expectation of Privacy: CDR/SAC		
Any support to Hostage Negotiations (Note 2)	Anywhere	Any Person or thing	CDR, USACIDC (in training situations)	Local Post Commander (real situations)	AR 190-30 FC 19-11
Forensic aids (Evidence processing or collection)	On post CONUS or OCONUS	Any person or thing	As delineated in CIDR 195-1	Same	AR 195-1 CIDR 195-1 FM 19-20
	Off-Post CONUS	Subject	As delineated in CIDR 195-1		
		Not subject to UCMJ	As permitted by local SJA	Same	
	Off-post OCONUS	Any person or thing	As delineated by existing SOFAs	Same	

NOTES:

1. A court order may be required, depending upon the expectation of privacy of the subject being surveilled.

2. The recording of telephone calls to MP operations desks and to other operations centers set up to handle hostage-type incidents need only be approved by the post commander, “except in instances requiring immediate action…” – paragraph 3-21 and 3-22f, AR 190-30.

3. Use of civilian authorities to accompany CID agents in seizure of off-post evidence is strongly encouraged.

A court order may be required in this situation.

All non-consensual USACIDC pen register/trap and trace operations within the United States require an order from a Federal District Court. 7

Figure 23-1. Use Guide

CHAPTER 24

24-1
Scope

The USACIDC Forensic Science Officer (FSO) Program pertains to the functional specialty of forensic sciences particularly forensic pathology and medicine, with an emphasis on death and sex crimes investigations and associated crime scenes.

24-2
Program objective

The objective of the FSO Program is to optimize the criminal investigative posture of USACIDC by providing highly trained USACIDC investigators with state of the art forensic techniques and equipment to conduct, assist and monitor serious and sensitive investigations, especially death and sex investigations and associated crime scenes.

24-3
Personnel, training and utilization

a. FSOs will be warrant officer special agents selected for and trained IAW AR 621-1, Training of Military Personnel at Civilian Institutions. This entails earning a Masters of Forensic Sciences (MFS) degree from the George Washington University and completing a Forensic Medicine Fellowship at the Armed Forces Institute of Pathology, which includes various short courses in the forensic sciences and completion of an original research project.

b. For FSOs in Army Educational Requirements System (AERS) validated positions, continuing education will, as a minimum, include attendance at the annual American Academy of Forensic Sciences meeting. Additionally, each FSO will attend at least 40 hours of training every two years. Resources permitting, other continuing professional development opportunities should be attended as required to meet their responsibilities. They will also be afforded the opportunity for continuing professional development throughout their assignments.

c. FSOs will be assigned to AERS validated positions. Personnel trained as FSOs must, IAW AR 621 -1, serve three years in a "utilization tour". To the extent possible, FSO responsibilities should be focused on their respective areas of functional expertise. They should not be assigned duties which interfere with responsibilities outlined in this regulation.

d. Funds to support field element forensic science and technical services operational and training responses will be provided by the parent unit.

24-4
Responsibilities

a. HQUSACIDC

(1) The Deputy Chief of Staff for Operations (DCSOPS):

(a) Establishes policy and provides oversight to the USACIDC FSO Program.

(b) Oversees FSO training programs and sets minimum training standards for FSOs, as well as training required to implement new techniques.

(2) The Deputy Chief of Staff for Support (DCSSPT):

(a) Assures properly trained personnel are assigned to forensic science positions.

(3) HQUSACIDC Forensic Science Officers:

(a) Advise the DCSOPS in matters pertaining to the application of the forensic sciences in the investigative and legal processes.

(b) Act as the primary criminal investigator liaison officers between USACIDC and the Armed Forces Medical Examiner’s Office. Optimize expenditure of Army resources in death cases through direct, two-way communication between USACIDC and the Armed Forces Medical Examiner’s Office.

(c) Review investigations, with particular emphasis on investigations involving crimes against persons, for investigative sufficiency and to assure applicable forensic techniques are used in the conduct of USACIDC investigations.

(d) Act as the primary criminal investigation liaison officer between USACIDC and the Office of the Judge Advocate General (OTJAG) for death and sex crime related cases. Optimizes expenditures of Army resources in sex crime cases in coordination with OTJAG. Ensures continuing integration of training of OTJAG and USACIDC personnel in the area of sex crimes.

(e) Review all initial and status reports pertaining to crimes against persons investigations, identifying areas of concern to field elements, as well as possible investigative techniques and equipment that could be employed.

(f) Coordinate forensic science training programs for USACIDC special agents with the Training Branch, HQ USACIDC.

(g) Mentor agents attending the Forensic Medicine Fellowship and monitor completion their research projects.

(h) Coordinate announcements, applications and nomination board for PERSCOM selection to The George Washington University.

(i) Represent USACIDC on the DA Family Advocacy Committee and Victim-Witness Assistance Council.

(j) Represent USACIDC on the DoD Forensic Science Committee.

(k) Attend DoD Family Advocacy Command Assistance Team (FACAT) training.

(l) Provide nominations for other CID agents to attend DoD FACAT training and then monitor their assignments and FACAT deployments.

(m) Provide support to field FSOs in the areas of consultation, on site assistance, and training or briefings so as to assure appropriate forensic techniques are used in the conduct of USACIDC investigations.

(n) Conduct liaison with investigative, legal, scientific, and medical professionals to assure their effective cooperation in forensic matters.

(o) Conduct investigative or investigative support operations which require forensic sciences expertise and direct involvement of HQ USACIDC investigators.

(p) Serve as the USACIDC Violent Criminal Apprehension Program (VICAP) Coordinator.

(q) Serve as supervisor of the Cold Case Squad, overseeing the development and completion of leads and conducting liaison with other investigative agencies, legal systems and forensic professionals to ensure successful resolution of investigations.

(r) Make recommendations for policy changes as needed.

b. USACIL

(1) The Director chairs the DoD Forensic Science Committee in accordance with guidelines established by the DoDIG, in accordance with DoD Instruction 5100.86, DoD Forensic Science Committee.

(2) The USACIL FSO:

(a) Advises the USACIL Commander in matters relating to the application of forensic science in investigative and legal processes.

(b) Monitors the technical aspects of USACIDC's Forensic Science program, to include reviewing the application of forensic science and law enforcement equipment and techniques to assure it is consistent with the investigative mission.

(c) Monitors policy associated with the application of the forensic sciences as well as use of forensic science and law enforcement equipment and techniques to assure it is consistent with investigative, legal, and administrative requirements.

(d) Makes recommendations for policy changes when needed.

(e) Identifies and evaluates forensic science oriented training, forensic science and law enforcement equipment and techniques, and other expert services suitable for use by USACIDC.

(f) Provides referrals to training and forensic analysis capabilities as well as other professional expertise needed to meet investigative requirements.

(g) Provides on-site operational and training support in the forensic sciences or finds resources to provide that support when requirements are beyond that available in the field or at the USACIL.

(h) Conducts liaison with investigative, legal, scientific and medical professionals, as well as vendors of investigative equipment and supplies.

(i) Stays current in the forensic sciences through review of professional literature, self study, and continuing education to include attendance at professional meetings such as the annual meeting of the American Academy of Forensic Sciences.

c. Commanders at all levels:

(1) Manage organic forensic science assets to assure USACIDC realizes the full potential of their expertise and the Army maximizes the return on the investments made to train these personnel. This includes assuring the FSOs are consulted in investigations where their expertise would be helpful in resolving the matter under investigation and assuring effective use of unit coordinators in training of personnel under their command.

(2) Promote the use of applicable forensic science techniques in the conduct of all investigations under their control.

(3) Provide resources necessary to support training and operational use of FSOs.

d. Field FSOs.

(1) On the direction of the battalion/district Operations Officer, respond to crimes scenes within their area of responsibility, providing assistance to the crime scene processing team(s) and advice to the Special Agent in Charge (SAC) or Task Force Commander (TFC).

(2) Act as the unit sex crimes expert, providing advice to the Operations Officer, the SAC(s) and special agents as needed.

(3) Review investigative reports, with particular emphasis on investigations involving crimes against persons, for investigative sufficiency and to assure applicable forensic techniques are used in the conduct of USACIDC investigations. Assist the SAC and operations officer in determining when equivocal deaths should be submitted to the OAFME for the possible initiation of a forensic psychological autopsy.

(4) Provide training to supported agents, Staff Judges Advocate and installation Medical Treatment Facility personnel on forensic capabilities of USACIDC, including USACIL. Support field investigators in the areas of consultation and training or briefings to assure appropriate forensic techniques are used in the conduct of USACIDC investigations.

(5) Contribute to selection screening process for applications to the George Washington University.

(6) Attend DoD FACAT training.

(7) Provide nominations for other CID agents to attend DoD FACAT training and then monitor their assignments and FACAT deployments.

(8) Conduct liaison with investigative, legal, scientific, and medical professionals to assure their effective cooperation in forensic matters.

(9) Review VICAP reports prior to submission to the FBI.

e. The USAMPS Chief of Physical Evidence:

(1) Reviews selected investigations, with particular emphasis on investigations involving crimes against persons, to ensure applicable forensic techniques are taught during the Apprentice Special Agent Course training.

(2) Identifies and evaluates forensic science oriented training to ensure new techniques with an application to USACIDC are doctrinally accurate and comply with established USAMPS and TRADOC policies. Implements new training into USACIDC core training.

(3) Oversees or monitors the instruction of all USAMPS forensic related matters to USACIDC personnel.

(4) Contributes to selection screening process for applications to the George Washington University.

(5) Attend DoD FACAT training.

(6) Provide support to field investigators in the areas of consultation, on site assistance, and training or briefings so as to assure appropriate forensic techniques are used in the conduct of USACIDC investigations.

(7) Conduct liaison with investigative, legal, scientific, and medical professionals to assure their effective cooperation in forensic matters.

CHAPTER 25

25-1
Purpose

This chapter provides direction for the receipt, safeguarding, maintenance, dissemination and permanent storage of Army criminal investigative and military police records; the services of the Defense Clearance and Investigations Index (DCII) and the National Crime Information Center (NCIC); the receipt and processing of criminal records checks; and for granting or denying release and amendment of information contained in files originated and/or maintained by the U.S. Army Criminal Investigation Command (USACIDC).

25-2
Policy

The Commanding General (CG), USACIDC, is the Department of the Army (DA) authority for the maintenance and permanent storage of Army criminal investigative records, and the release of copies of USACIDC reports of investigation (ROIs), military police reports (MPRs) or information therefrom. DA policies pertaining to criminal investigation activities are outlined in Army Regulation (AR) 195-2, AR 190-30 and AR 190-45. AR 25-55 and AR 340-21 govern the Freedom of Information Act (FOIA) and Privacy Act (PA) functions, respectively. This chapter expands upon policies and establishes USACIDC investigative procedures relating to U.S. Army Crime Records Center (USACRC) services within the authority of the above-cited regulations.

25-3
USACRC responsibilities

a. Serve as the principal advisor to the CG, USACIDC, on the receipt, maintenance and retention of Army criminal investigative records within USACRC and on the dissemination and use of USACIDC and military police (MP) records within the Executive Branch of the Federal government or other law enforcement agencies.

b. Affect liaison with the Defense Security Service (DSS) and other Federal investigative agencies relating to the acquisition, maintenance, dissemination, and retention of criminal investigative records and information.

c. Administer the USACIDC FOIA/PA Programs.

25-4
Exceptions to policy

Requests for exception to policies and procedures expressed herein are within the headquarters staff responsibility of the Director, USACRC.

25-5
General

a. The USACRC service is based on the receipt and use of collected criminal investigative records information to solve ongoing criminal activity.

b. To enable the proper and accurate identification of criminal suspects who have committed prior criminal acts, it is essential that each special agent (SA) and USACIDC supervisor review all ROIs to ensure that names and personal identifying data entered into the Automated Criminal Information Reporting System (ACIRS) database is entered correctly and that USACIDC reports are transmitted to USACRC in a timely manner.

25-6
Information disclosure accounting by USACIDC investigative units

a Should a Department of Defense (DoD) element, or any Executive Branch law enforcement agency, desire a copy of a ROI subsequent to initial distribution, such release is authorized at the local USACIDC level in accordance with this regulation. Users of USACIDC or MP records for other than criminal investigative purposes or criminal justice disposition will retain USACIDC records in their possession the minimum length of time necessary, and destroy or return them to the local USACIDC investigative unit that provided the records (See AR 600-37). In cases of release of USACIDC records outside DoD, an original CID Form (CIDF) 118-E-R (Disclosure Accounting Record) will be forwarded to the Director, USACRC, documenting the release and citing the nature and purpose of the law enforcement agency receiving the report. The original CIDF 118-E-R will be forwarded with the final ROI, or forwarded separately if information is released subsequent to submission of the final ROI. Releases on CIDF 118-E-R that do not pertain to a ROI will be retained with the appropriate case file and not forwarded to the USACRC. Protective markings will not be cancelled on ROIs released to law enforcement agencies.

b Other releases of information in connection with FOIA/PA requests will be in accordance with section VII of this chapter.

25-7
Allocation of report numbers

a. The USACIDC report number is defined as a series of numbers which include a locally assigned four digit sequence number, a two digit year group, the unit identification number following the word “CID”, a five digit USACRC allocated ROI number, and the appropriate offense code(s) (i.e., 0001-99-CID001-00001-5C1B).

b. The ROI number is issued for use with initial, status, collateral, final and supplemental ROIs.

c. ROI numbers will be uploaded directly into each ACIRS computer and assigned in sequence as the respective USACIDC investigative unit dispatches each initial report.

d. Provost marshals (PM) and security officers are also allocated USACRC report numbers on an annual basis for those MPRs accessioned at USACRC in accordance with AR 190-45. These allocated report numbers also consist of a five digit number, but are configured with four numeric and one alpha character (i.e., 5000T). The overall MP report number is configured similar to USACIDC ROI number.

25-8
Accountability of reports of investigation

a. The USACRC forwards to USACIDC investigative units on a quarterly basis copies of registers (listings) of pending USACIDC cases, of those cases requiring disposition of offender reports, and a cumulative listing of all USACIDC cases opened and finalized during the calendar year. These listings are computer printouts prepared either by or for the USACRC. These documents may be used to supplement logs for all USACIDC investigative units, and to assist in maintaining the record copy of USACIDC reports at the USACRC. Following receipt of the pending, disposition and cumulative registers, one copy of each will be updated or corrected by pen and ink changes and returned to the USACRC within 45 business days. All changes will be updated in the local ACIRS database.

b. The Crime Records Division, USACRC, communicates directly with USACIDC investigative units for the purpose of correcting minor deficiencies identified during processing of reports.

25-9
Liaison activities

a. The USACRC maintains liaison with federal investigative agencies as it pertains to the exchange of criminal investigative reports or information in support of investigations within the Executive Branch. These agencies include, but are not limited to the following:

(1) Defense Security Service (DSS).

(2) U.S. Army Intelligence and Security Command (Investigative Records Repository).

(3) Department of the Army Suitability Evaluation Board.

(4) U.S. Army Central Personnel Security Clearance Facility.

(5) U.S. Army Military Police School.

(6) National Security Agency.

(7) Central Intelligence Agency.

(8) Federal Bureau of Investigation (FBI).

(9) Office of Personnel Management.

(10) Immigration and Naturalization Service.

(11) Department of State.

(12) Naval Criminal Investigative Service (NCIS).

(13) U.S. Air Force Office of Special Investigations (AFOSI).

(14) U.S. Treasury Enforcement Agencies (Internal Revenue Service, Secret Service, U.S. Customs, Bureau of Engraving and Printing, Alcohol, Tobacco and Firearms).

(15) Defense Criminal Investigative Service.

b. The USACRC maintains liaison with various DoD elements as it pertains to the exchange or dissemination of ROIs, MPRs, or criminal history information that is compatible with the purpose for which such records are acquired and maintained.

c. All USACIDC investigative units at all levels are authorized and encouraged to contact the USACRC for the purposes of obtaining investigative information from reports or in coordinating information with the agencies listed in paragraph 25-9a, above.

25-10
General

One of the primary functions of the USACRC is to receive and disseminate information relative to criminal activities to authorized requesters on a 24-hour basis. These requests fall into one of two categories; "Immediate Action" or "Routine." When feasible, records/name checks should be accomplished prior to the interview of suspects and/or victims.

25-11
Immediate action records/name checks

Several methods; telephone, electrical message, facsimile transmission and ACIRS electronic mail (email) receive immediate action records/name checks.

a. Telephonic requests:

(1) Telephonic requests may be made to the USACRC on a 24-hour, seven days a week basis. Telephone requests should not normally exceed five names. Dependent upon the availability of records, a search will be conducted while the requester waits on the telephone. In the event the requested information is not immediately available, the information will be provided expeditiously by telephone.

(2) All telephonic requesters will be required to identify themselves in accordance with AR 195-2 and provide the USACRC with the report number with which the request is associated. If a report number has not been assigned, the requester will provide some other means of identification.

(3) The SA requesting the telephonic name check will ensure that the following information is recorded in the case file's agent activity summary (AAS):

(a) Time and date the request was made.

(b) Name of the person who made the request.

(c) Name of the person on whom the check was made.

(d) Results of the records/name check.

(4) If the offense for the telephonic request is murder, rape, robbery, indecent acts against a child or certain white-collar crimes, the NCIC system will also be queried.

b. Electrical message. Message requests will be addressed to the DIR USACRC USACIDC FT BELVOIR VA //CICR-ZA//. These electrical messages, which are not associated with initial or status ROIs, should contain:

(1) Name of individual listed in request.

(2) Date of birth.

(3) Place of birth.

(4) Social Security Account Number (SSAN).

(5) Report Number.

(6) Purpose for the records/name check (i.e., employment as a childcare provider or criminal investigation).

(7) Agent sequence number and name of individual preparing the request.

c. Email.

(1) Records/name check requests may be forwarded to the USACRC via email addressed to the USACRC organizational mail account, mailcicn@acirsf.belvoir.army.mil. Requests must contain the same information as detailed in paragraph 21-11b. Questions regarding the status of an email request, operational problems, or requests for additional information should be directed to mailcicr@acirsf.belvoir.army.mil.

(2) In-coming requests are forwarded to "mailboxes" within the Records Retrieval Branch, USACRC. Requests on childcare providers are queried through the DCII, the Automated System Crime Records Center (ASCRC), and the ACIRS database. Other requests are handled as routine records/name checks, unless otherwise specified.

(3) Once the records/name checks are conducted, the files are retrieved and summarized and a message sent back to the requesting investigative unit via ACIRS Email.

(4) The USACRC can conduct records/name checks where the only identifier is a name. However, requesters are advised that records on subjects with

common names often require additional identifiers to ensure retrieval of the correct record(s).

(5) A records/name check of suspects listed in initial and status ROIs will receive priority. Derogatory information developed as a result of initial and status ROIs will be forwarded to the requester via e-mail.

d. Records/name checks conducted relative to subjects of requests for polygraph examination authorizations will be treated as immediate action requests, with the results and/or case files presented to the polygraph approving authority for review.

e. Records/name check request from external agencies.

(1) Under no circumstances will a records/name check be made based on a request from any person or organization not listed in the applicable Privacy Act Systems Notices of DA Pam 25-51 and this regulation, except with the written consent of the individual being checked. Disclosure of records/name check information to other than routine users of law enforcement information, without the written consent of the person in question, is prohibited.

(2) Requests from any law enforcement agency to USACIDC investigative units will be recorded on a CID Form 66 (USACIDC Action Record) with a brief justification for the request.

(3) In addition to recording the information required in subparagraph 21-11a(3), the release outside DoD of the results of records/name check will be recorded on CIDF 118-E-R, in accordance with section VII of this chapter.

25-12
ASCRC

When a records/name request emanates from Army law enforcement authorities, the ASCRC will automatically be searched. Information prior to 1 July 1992, contained in this index, provides indices to probable cause contained in unfounded, insufficient evidence, and juvenile cases, which is generally releasable only to Army law enforcement in accordance with applicable USACIDC system notices contained in DA Pam 25-51 and AR 195-2. Subsequent to 1 July 1992, under new titling procedures, subjects of unfounded, insufficient evidence, and juvenile cases remain indexed in the DCII. Requests for exceptions to this policy will be addressed to the Director, USACRC.

25-13
Routine records/name checks

Routine requests for records/name checks are those received through letters or other correspondence. Requests will normally be answered in the media in which they were received, (i.e., mail by mail and message by message). Requests described in this paragraph should contain the same information as noted in paragraph 25-11b.

25-14
Records checks in support of the U. S. Total Army Personnel Command (TAPC) Activities, General Officers Management Office (GOMO), Office of the Sergeant Major of the Army, and Senior Executive Service (SES) personnel screenings

a. The procedures outlined here govern the USACRC records screening of personnel under consideration for employment in the SES, as members of a variety of DA boards, those selected for promotion to certain ranks, those identified for certain command positions, and other records/name checks deemed appropriate. All information provided as a result of these checks will be at the direction of the CG, USACIDC, and may include any information accessible by the USACRC.

b. Procedures: The USACRC receives a name or listing of names to be checked with a point of contact from the requesting office. The names will be checked through the DCII and the indices of the investigative databases of the USACIDC for investigative records. The Director, USACRC; Deputy Director, USACRC or Chief, Crime Records, to validate that the investigative results were properly classified as either "founded" or "unfounded", will review all record identified. Only those cases classified as "founded" will be provided.

c. Further processing of developed information will be as follows:

(1) Support of the TAPC - Founded Army criminal investigative reports will be reproduced in whole or in part and provided to the TAPC by the USACRC. A copy of the correspondence being returned, less copies of the investigative reports, will be forwarded to the CG, USACIDC, for information.

(2) Support for the GOMO - Founded Army criminal investigative reports will be summarized and reproduced. Correspondence bearing the CG, USACIDC's signature block, with the summaries enclosed, will be prepared and copies of the pertinent reports will be provided as additional backup information in the event additional questions arise. This information will be on a "Close Hold" basis and

will be handled between the USACRC and the CG, USACIDC's secretary, aide, or the Deputy Commander (DCO), USACIDC. Correspondence will be hand carried by USACRC representatives.

(3) Support of SES Screening - The same procedures will apply as for processing GOMO requests, with the exception that the primary signature block to report the summaries will be that of the DCO, USACIDC.

(4) Support for Office of the Sergeant Major of the Army - Listings of Command Sergeants Major (CSM) nominated for General Officer CSM slates will be provided by the TAPC CSM/SGM Branch. Founded Army criminal investigative reports will be reproduced in whole or in part and provided to the Office of the Sergeant Major of the Army by the USACRC. The TAPC will receive correspondence from the USACRC confirming only that the checks were completed and that the results were provided to the Office of the Sergeant Major of the Army.

25-15
Procurement of files

a. ROIs, MPRs, and reports generated by the AFOSI, NCIS, and the FBI, involving U.S. Army personnel or property, which have been forwarded to the USACRC for permanent filing, are immediately available for review and transmittal to USACIDC and MP requesters on a 24-hour, seven day per week basis.

b. U.S. Army Intelligence dossiers and DSS files are not normally accessible to the USACRC during non-duty hours.

c. Requests for DSS, AFOSI and NCIS files should be addressed to the Director, USACRC.

25-16
Intelligence files procurement

Each USACIDC major subordinate command will appoint two file procurement officers in accordance with AR 381-45 to obtain intelligence dossiers from the Investigative Records Repository (IRR), U.S. Army Intelligence and Security Command (INSCOM), Fort Meade, MD. Written requests for the file procurement officer will forward dossiers needed in criminal investigations to the Director, USACRC, or by ACIRS e-mail, from where they will be relayed to the IRR. The IRR will then forward the dossiers directly to the file procurement officer. Users will retain the dossiers in their possession the minimum length of time necessary,

and then return them directly to the IRR. A continuous chain of receipt will be maintained for dossiers by USACIDC investigative units.

25-17
Use of the National Crime Information Center (NCIC)

a. The NCIC is a computerized index on criminal history, fugitives (to include military deserters), and identifiable stolen articles. The NCIC is maintained by the FBI for use by all law enforcement. Within the U.S. Army, on-line computer terminals are available at the Army Deserter Information Point (USADIP), the USACRC, and the continental United States (CONUS) installation Provost Marshal Offices (PMO) Army deserter information is entered into the files of the NCIC by the USADIP. All lost or stolen U.S. Army weapons are entered through CONUS Army terminals. Detailed instructions on the operation and use of the NCIC are prepared by the FBI and are available at each computer terminal. The DA policy is contained in AR 190-9 and AR 190-27.

b. Each USACIDC major subordinate command within CONUS will, in coordination with the agency responsible for the operation of the nearest NCIC terminal, establish procedures to ensure maximum utilization of the NCIC. If primary investigative responsibility rests with the USACIDC, entries into the NCIC will be as follows:

(1) Stolen U.S. Government vehicles and stolen privately owned vehicles.

(2) Stolen or lost U.S. Government weapons and stolen privately owned weapons will be entered by the local PM in accordance with AR 190-11.

(3) Serial numbered stolen property, either U.S. Government or privately owned, of any value, if the theft is being investigated by the USACIDC.

(4) Serial numbered securities, which have been stolen, counterfeited or lost. The term "securities" includes currency (bank notes, bills, etc.), bonds, debentures, notes, common or preferred stock certificates, traveler’s checks, money orders, or U.S. Treasury checks.

c. All entries made through CONUS terminals will contain the entry "Call Army USACIDC (area code and phone number)" in the miscellaneous field. The phone number of the investigating USACIDC investigative unit will be used in this entry.

d. Army personnel in a deserter status who are listed as subjects of ROIs will be entered into the NCIC by the USACRC. This action is accomplished upon receipt of the action copy of the ROI required by section IV of this chapter.

e. Felony warrants and temporary USACIDC "wants" may be entered into the NCIC prior to receipt of the final ROI, in accordance with this regulation.

f. Validation of all NCIC entries will be accomplished by the supporting NCIC field terminal in accordance with schedules announced by the FBI. All USACIDC investigative units making NCIC entries will participate in such validations when requested by the NCIC field terminal responsible for making the NCIC entry. The validation process will include a review of each open entry to ensure that the item is still being sought, that all information is current and accurate, and that the records contain all available descriptive data.

g. All USACIDC investigative units located outside CONUS (OCONUS) will make entries into the NCIC concerning stolen property, meeting the criteria in paragraph 25-17b above. This information will be provided to the USACRC by e-mail for entry through the NCIC computer terminal at that site.

mailcicr@belvoir.army.mil.

h. A ROI number is required for all USACIDC NCIC entries.

25-18
Computerized Criminal Histories (CCH)

a. General. The CCH is a computerized database containing criminal histories. Entry into the CCH and the Interstate Identification Index (III) is accomplished through the U.S. Army NCIC/CCH control terminal at the USACRC. Operation of this terminal will be in accordance with concepts, policies and procedures established by the FBI, NCIC Advisory Policy Board and adopted by the NCIC.

b. Responsibilities.

(1) The Chief, Security, Force Protection and Law Enforcement Division, Deputy Chief of Staff for Operations, HQDA (DAMO-ODL), is responsible to the FBI NCIC to ensure information derived from NCIC/CCH is used only for official purposes.

(2) The CG, USACIDC, is responsible for establishing internal CIC/CCH procedures and implementing rules and policies consistent with the policies approved by the NCIC Advisory Policy Board and DAMO-ODL.

c. Operational Procedures.

(1) Direct access to the CCH computerized files by USACIDC investigative personnel will be permitted only in the discharge of official duties.

(2) Queries of the CCH system will be made only in support of criminal investigations and will not be used for crime surveys or application for employment.

(3) All CONUS, requests for CCH checks will be submitted to the supporting PMO in accordance with local procedures Requests for exceptions to this policy (i.e., remote CONUS USACIDC offices not located with a PMO) may be submitted to the Director, USACRC, ATTN: CICR-CR. All CCH requests should include the subject's full name, aliases, social security number, date and place of birth.

(4) All OCONUS requests for CCH checks may be submitted to the Director, USACRC by telephone, e-mail or memorandum. The USACRC response to matching records in the NCIC will be limited to a mailed copy of the NCIC printout. Exceptions may be made when there is an immediate need for this information to further an investigation, or there is a situation affecting the safety of law enforcement or the general public. Requests for USACRC CCH checks meeting the above criteria must clearly state this requirement.

(5) All USACRC provided CCH printout sheets must be destroyed (shredded or burned) when it has served the purpose for which it was requested. These documents may not be copied or faxed. The information contained in the printout may be transcribed and included in the ROI, if appropriate.

25-19
General

The "USACIDC Wanted" Deserter System is a procedure to effect the apprehension of deserter felons/suspected felons through the entry of their names and personal identifiers into the NCIC. The USACRC is the USACIDC centralized holder of ROIs in which the subject/suspect or other key individuals are in deserter status, and returns those cases to the originating USACIDC investigative units upon the return of the individual to military control. These procedures accomplish the following:

a. Alerts civilian and military law enforcement agencies of the felony offense so that appropriate precautions may be taken in the apprehension of the subject/suspect.

b. Upon apprehension of the subject/suspect, USACIDC investigative units can prepare a supplemental ROI to document the return of the subject/suspect to military control and the completion of remaining investigative leads.

25-20
Crime Records Center Procedures

a. Upon receipt of an initial, status or final ROI with supporting documentation reflecting the subject/suspect to be in deserter status, the USACRC will insure that a "USACIDC Want" tag-on entry is effected to the USADIP entry pertaining to the deserter.

b. The USACRC, when advised by competent authority that the subject/suspect has been returned to military control, will telephonically verify the presence of the individual at the location reported. Return of previously closed ROIs will be as follows:

(1) Final ROIs (military member is still on active duty): Telephonic or e-mail notification will be made to the originating USACIDC investigative unit. A copy of the ROI will be returned to the originating unit by memorandum of transmittal (MOT) for appropriate action if the local case retention period has terminated. Overnight or express mail delivery of the MOT/ROI may be used when appropriate. A copy of the MOT/ROI will be forwarded to the USACIDC investigative unit having operational jurisdiction at the location where the individual was returned to military control to facilitate investigative activity. Investigative units will establish their own procedures as to how best to complete pending investigative leads.

(2) Final ROIs (military member discharged prior to action being taken): A copy of the ROI, less exhibits, will be returned to the originating USACIDC investigative unit by MOT for preparation of a supplemental ROI if the local case retention period has terminated. It is suggested that the results of the investigation pertaining to federal violations be furnished to the appropriate civilian federal investigative agency for the purpose of determining the feasibility of prosecution in U. S. Federal Court. A copy of the complete ROI should be provided to the Director, National Personnel Records Center, 9700 Page Avenue, St. Louis, MO 63132, to be included in the subject's personnel file for consideration in any future personnel actions, to include future acceptance into any of the military services.

c. All USACIDC investigative unit supervisory personnel should ensure that an individual, on which a “CID Want" tag-on entry is to be made, is truly "wanted" by the USACIDC. All ROIs finalized, with unknown subjects which previously had "CID Want" tag-on deserter entries into the NCIC for suspect personnel, will cause the "CID Want" tag-on entry to be cleared from the NCIC, unless the status section reflects the suspect is still wanted by the USACIDC. The definition of suspect as reflected in this regulation will be followed judiciously when requesting that a "CID Want" tag-on entry be placed in the NCIC.

25-21
General

This section prescribes the purpose and responsibilities for referral of Criminal History Information (CHI) received by the USACRC from DSS, INSCOM, and other investigative agencies of the Federal government. This information is received from Entrance National Agency Checks (ENTNAC), National Agency Checks (NAC), expanded NACs, security investigations, background investigations, FBI record of arrests (Rap Sheet), or criminal investigations by other Federal law enforcement agencies wherein information was developed of a criminal nature pertaining to a member of the Army or Army property. These records, investigations and sources of information are referred to as “source documents”.

25-22
Purpose

a. The primary purposes for the referral of CHI received from a source document are:

(1) To establish modus operandi files to assist in the investigation and prevention of offenses within the recipient's area of responsibility.

(2) To identify prospective sources of information in the recipient's area of jurisdiction.

b. The referral of CHI, other than that specified above, will reflect the specific action desired and whether a reply is necessary.

25-23
Procedures

a. The Crime Records Center will:

(1) Obtain from DSS those ENTNACs warranting referral to USACIDC investigative units.

(2) Maintain source documents in suspense until the individual arrives at the first permanent duty station.

(3) Refer derogatory source document to the USACIDC investigative unit located at the individual's present or next scheduled permanent duty station. Electronic or automated transmission of this information is encouraged.

(4) Refer all other items of criminal activity obtained from other investigative agencies as received.

b. All USACIDC investigative units will:

(1) Implement a file (i.e., modus operandi or alphabetical) of the derogatory source documents for the purposes cited in paragraph 25-22.

(2) Maintain derogatory source documents in their criminal information system.

(3) Retain derogatory source documents for three years, or until the individual departs that installation. At that time, the source documents will be destroyed.

(4) Act upon those referrals of criminal activity which are cited in paragraph 25-22(b).

25-24
General

The DCII is a computerized information database located at the Personnel Investigations Center (PIC), DSS, Baltimore, MD. Conceptually, the DCII is analogous to a library reference card catalog. The DCII reflects only the existence and location of a particular type of file and not the contents of that file. The DCII keys on the Personal Identifying Data (PID) (name, SSAN, POB, DOB) that is inserted by the contributing component. The DCII was established in concept by the Secretary of Defense in 1966, as the central index for all military departmental investigations. Requesters are numerous and include authorized DoD activities and Federal agencies.

25-25
Concept

a. The DSS maintains the DCII solely to expedite the investigative process and to ensure that all investigative agencies are alerted to current or previous investigations of individuals.

b. Detailed instructions on the operation and use of the DCII are prepared by the DSS and contained in a DCII users' manual available at each computer terminal located at the USACRC. The DA policy on the DCII is detailed in AR 195-2.

c. The DCII includes index tracings to:

(1) Subjects of ongoing ROIs.

(2) Subjects and victims, to include juveniles, of finalized ROIs.

(3) Subjects of completed MPRs provided to the USACRC.

(4) Other criminal, intelligence and personnel security files maintained in the repositories of the NCIS, AFOSI, DSS, INSCOM, and Department of Defense Inspector General (DoDIG).

26-26
Control

Except as required by law or directed by competent authority, the CG, USACIDC, has control over any and all portions of the DCII that index or otherwise pertain to Army law enforcement records.

a. This authority specifically includes control over the criteria governing the insertion and deletion of information in the DCII, and the contents of insertions and the scope of deletions.

b. All such information remains the property of the USACIDC, irrespective of the fact the data is maintained by DSS in the DCII.

25-27
Responsibilities

a. The CG, USACIDC, is responsible for the accuracy and propriety of all personal information extracted from USACIDC records and inserted and maintained in the DCII. The Director, USACRC, is delegated the authority to insert, delete and/or expunge USACIDC criminal investigative indices in the DCII, in a manner consistent with the CG, USACIDC’s guidance.

b. The Director, USACRC, is responsible for all insertions into and/or expungements from the DCII and indexing data from other law enforcement records on file at USACRC in a manner consistent with HQDA guidance.

c. The Director, USACRC, is responsible for the insertion of all personal information on juvenile suspects, subject or victims identified in USACIDC records into the DCII in accordance with DoD instructions 5505.7.

d. The Director, USACRC, maintains internal procedures to implement the provisions of the DCII users' manual in a manner consistent with policies prescribed herein or by higher authority.

25-28
DCII insertion/deletion procedures

a. The Director, USACRC, will:

(1) Upon receipt of an initial ROI, insert into the DCII an open case (ongoing) entry consisting of the ROI number and available PID on all suspects/subjects.

(2) Upon receipt of a status ROI that deletes a suspect from the subject block of a ROI, immediately delete from the DCII the former suspects/subject PID and have it entered into the ASCRC. See paragraphs 7-4a and 25-34c.

(3) Upon receipt of a status ROI that inappropriately deletes a suspect/subject from the subject block, immediately direct that the appropriate USACIDC investigative unit prepare a supplemental message ROI adding the suspect/subject and providing investigative explanation clarifying that the allegation(s) was determined to be unfounded or that there was insufficient evidence to prove/disprove the subject committed the offense(s) under investigation.

(4) Upon receipt of an initial/status message ROI with restricted distribution requirements (See chapter 7), immediately inserted suspect/subject PID into the ASCRC only and not the DCII.

d. Upon receipt of the final ROI:

(1) Insert into the DCII a final case entry of the PID of all suspects, subjects and victims, to include juveniles.

(a) As of 1 July 1992, all subjects, suspects, victims, organizations, corporations and juveniles, previously indexed in the ASCRC only, will be entered into the DCII with the following survey codes:

1. X - Unfounded

2. E - Insufficient Evidence

3. J - Juvenile

(b) Restricted and polygraph only cases will continue to be entered into the ASCRC only.

(2) Delete from the DCII the appropriate pending case entries.

e. Upon receipt of properly referred MPRs, insert or delete from the DCII in accordance with the specific written direction of the Office of the Deputy Chief of

Staff for Operations (ODCSOPS). The policies of ODCSOPS shall be complied with by USACRC insofar as they are not inconsistent with law, regulation or workload requirements.

f. Delete from the DCII those tracings or portions thereof pertaining to a ROI as determined proper under law or regulation. This applies primarily to ROIs closed prior to 1 July 1992. Subjects of ROIs closed subsequent to 1 July 1992, may be deleted from the DCII only as a result of mistaken identity or when an error occurred in applying the credible information indexing standard. (See paragraphs 7-4a and 25-34c).

g. Use of the DCII tracing in USACIDC name check procedures (section III) is limited only to signaling that a case file exists and its location. Release of information for name check purposes will be from the actual case file.

h. Copies of case files from DSS and Army Intelligence are automatically requested by the USACRC for use by USACIDC investigative units when the DCII tracing reflects the existence of a file. The USACRC will obtain copies of other agency reports upon request only.

i. Exact PID information is crucial to obtaining a useful DCII tracing. Although partial data inquiries can, on occasion, be successful, it is essential that PID information be as accurate as possible to preclude erroneous entries and tracings.

25-29
Release of information

a. Release of DCII tracing information, whether related to a ROI or other component originating tracing, is subject to the restrictions of the PA, AR 340-21, AR 195-2 and this chapter.

b. Tracings or information pertaining to ongoing USACIDC investigations are generally releasable only to Army law enforcement authorities.

c. Tracings or information pertaining to final ROIs are releasable only in accordance with AR 195-2, AR 25-55 and AR 340-21.

25-30
General

This section sets forth policies and procedures for the processing of requests for the release and amendment of records contained in files originated or maintained by the USACIDC under the FOIA/PA.

25-31
Policies

a. The USACIDC will release requested information to the maximum extent possible, consistent with applicable laws and regulations.

b. Requests may not be denied by any person other than the CG, USACIDC, or specifically designated representatives. All FOIA/PA and amendment requests for USACIDC originated or maintained information will be referred immediately to the Director, USACRC. Requesters will be advised of the referral.

c. When requested USACIDC records include information originated by another organizations, a copy of the request, along with the non-USACIDC originated information/documents will be forwarded to the originating organization to act on the request, if the originating source is known. Generally, the referral will be for direct reply to the requester.

d. Unless otherwise restricted, disclosure of USACIDC originated criminal investigative records to routine users is authorized for criminal law enforcement purposes. Routine users are those organizations described in the system notice applicable to the records from which the disclosure is to be made.

25-32
Control

a. Disclosure is authorized to those persons or components within DoD who have an official need for the USACIDC record in the performance of their duties, when the intended use is compatible with the purpose for which the USACIDC record is maintained. These two general conditions are presumed to be satisfied, if such disclosure is specifically required or authorized by regulation.

b. A USACIDC investigative unit may not disclose outside DoD channels any records or information originated by another organization that may be exempt under the FOIA/PA, unless prior approval has been obtained from the originating organization. For example, FBI reports, Inspector General (IG) reports or medical records may not be disclosed outside DoD channels, even though they may be exhibits in a ROI, unless prior approval has been obtained from the originating organization or authorization is provided by regulation.

c. All USACIDC investigative units will normally refer requests for release of information to the Director, USACRC; however, investigative units may obtain authorization to release records directly to a requester by obtaining prior telephonic or written authority from the Director, USACRC.

d. Disclosure Accounting Record. All USACIDC investigative units will prepare CIDF 118-E-R for all disclosures of personal information made to persons or organizations outside the DoD. However, if for example, during the course of a USACIDC investigation, information is exchanged with the FBI over a period of several days, a single entry on CIDF 118-E-R that describes the on-going manner in which information was disclosed will suffice. The original CIDF 118-E-R will be forwarded to USACRC as an attached exhibit for filing with the final ROI. CIDF 118-E-R pertaining to actions completed on non-ROI activities will not be forwarded to USACRC but will be retained with the original case file.

e. Request from Courts, Boards, and Trial/Defense Counsel.

(1) All USACIDC investigative units will forward a copy of all requests, orders or subpoenas from any civilian court or regulatory body (including defense and prosecutorial requests, juvenile and probation proceedings) for USACIDC maintained information to the Director, USACRC, ATTN: CICR-FP. The forwarding investigative unit will also provide information required by AR 27-40, if such information has not been provided previously to the Judge Advocate General by the local servicing staff judge advocate (SJA).

(2) All USACIDC investigative units will comply with orders issued by a military court for the production of any USACIDC maintained records/information, unless a USACIDC supervisor believes that the request should be forwarded for decision to the CG, USACIDC.

(3) Other requests for USACIDC maintained information (including defense counsel requests), during the course of an Article 32, UCMJ investigation or other military judicial or administrative proceedings, normally will be honored, if the servicing SJA agrees. If the servicing SJA advises to the contrary, or the USACIDC supervisor believe the release of the requested information should be denied, the request should be referred to the USACIDC major subordinate command judge advocate (JA) for resolution.

(4) The SJA or trial counsel normally will be provided any USACIDC maintained information necessary to carry out their military justice responsibilities. If agreement cannot be reached between the local USACIDC supervisor and the local SJA or trial counsel, the USACIDC supervisor should consult the USACIDC major subordinate command JA for guidance.

(5) Requests from other than a military judge to disclose the identity of a USACIDC source will only be honored after consultation and agreement between the USACIDC supervisor and the SJA. If agreement cannot be reached, the USACIDC supervisor will withhold release of the information and immediately forward the request to the USACIDC major subordinate command JA.

f. Congressional and White House Inquiries. Congressional or White House inquiries will be handled in accordance with CIDR 1-20. Normally, HQUSACIDC will prepare all responses to Congressional inquiries relating to USACIDC activities.

g. Obtaining SSAN

(1) The SSAN may be requested directly from an individual, provided the individual is first informed of the following:

(a) The SSAN is requested under the authority of Executive Order Number 9397, 22 Nov 43; 10 USC 3012 (for DA Forms) or 5 USC 301 (for other forms).

(b) The SSAN will be utilized to facilitate the definite identification of the individual who is supplying information to USACIDC, pursuant to the request of its special agents during the course of criminal investigative activities.

(c) The furnishing of the SSAN is voluntary, but if the individual refuses to disclose the number, USACIDC personnel will obtain the number from official federal agency records.

(2) The military identification card (DD Form 2) should not be requested for the sole purpose of obtaining a SSAN. If the ID card is requested legitimately and in good faith for other purposes, such as verifying that person's identity when the person has refused to provide adequate identification, then the SSAN may be acquired from the ID card.

(3) The PA requires, under penalty of criminal or civil sanction, that actual notice be provided to the individual whenever soliciting a SSAN. It is not deemed necessary that the individual be given a copy of the notice, nor is a signed acknowledgment of such advice required to be retained by the USACIDC.

h. Privacy Act Statement:

(1) Because of the general exemption status granted for USACIDC investigative record systems, DA forms used to obtain personal information acquired for and ultimately maintained in those systems of records are generally exempt from the requirement to use a privacy act statement. The USACIDC forms are similarly exempt from the requirement for a privacy act statement when the forms were specifically designed for the identification or investigation of criminal activity. The general exemption does not eliminate the requirement to advise persons of the information in paragraph 25-32g(1) prior to requesting their SSAN.

(2) Privacy act statements are required on USACIDC forms which are used to collect personal data for non-investigative purposes.

i. Information furnished by Foreign Sources: Foreign governments that furnish information relevant to DoD criminal investigations are concerned with disclosure. The following guidance is provided concerning the protected status such information may be given:

(1) Information received with a security classification assigned by a foreign governmental source will be brought under control and assigned a corresponding U.S. Government security classification, assuming such information can be classified properly pursuant to Executive Order 11652. The information will be protected from disclosure under both the FOIA and PA.

(2) Information received from a foreign governmental source which has not been assigned a security classification by the foreign or U.S. Government may also be protected under the FOIA and PA as information received from a source. Foreign governmental sources should be expressly advised that they may request and be granted status as a source if such foreign governmental source would otherwise refuse to provide the information.

(3) Information received from a foreign governmental source requesting confidential status will be clearly annotated “For Official Use Only” together with the fact, date, and by whom such assurances of confidentiality were given. Any USACIDC SA or supervisor obtaining information from foreign governmental sources may grant such express assurances of confidentiality.

j. Right to Financial Privacy Act of 1978, (12 USC 3401). USACIDC records containing information obtained from a financial institution may be subject to the restrictions of the Right to Financial Privacy Act of 1978. Disclosure of such records outside of DoD must be coordinated with the major subordinate command JA or HQUSACIDC SJA prior to disclosure to ensure compliance with the requirements of that act.

k. Specific issues not adequately covered by this chapter may be directed to the appropriate major subordinate command JA; Director, USACRC; or the HQUSACIDC SJA for resolution.

25-33
Responsibilities

a. The CG, USACIDC, has overall responsibility for the release of information and serves as the USACIDC Initial Denial Authority (IDA) under the FOIA and as the Access and Amendment Refusal Authority (AARA) under the PA to deny, in whole or in part, access to or amendment of information from USACIDC criminal investigative reports, MPRs, and other files originated and/or maintained by the USACIDC under AR 195-2, AR 190-45, AR 25-55 and AR 340-21.

b. The Director, USACRC will:

(1) Function as the principal adviser to the CG, USACIDC, on matters pertaining to the FOIA/PA; requests received from persons, non-media agencies and governmental organizations external to the Executive Branch, for non-routine uses of USACIDC records or information; and requests from routine users.

(2) Exercise staff supervision over the Chief, FOIA/PA Division, who is responsible for the implementation of policies concerning the FOIA/PA.

(3) Act as the custodian of USACIDC and MP reports, releases USACRC maintained investigative records to other USACIDC/MP investigative units, DoD components and agencies of the Executive Branch for routine uses authorized under the appropriate Privacy Act System Notice.

(4) Maintain accounting records of disclosures of information contained in USACIDC record systems maintained by the USACRC, as required by AR 340-21.

(5) Act as the proponent and provides technical advice on the release or denial of access to, or amendment of, polygraph records.

(6) Act as the proponent in the review of requests for access to, or amendment of Army criminal investigative reports.

(7) Act as custodian of USACIDC reports and prepares supplemental ROIs to effect approved amendments of reports not maintained in ACIRS.

(8) Act as custodian of MPRs and prepares supplemental MPRs to effect approved amendments of reports when the report is more than five years old.

(a) Information pertaining to the subject or victim of a report will be deleted from the report, removed from the DCII and added to the Identification Index.

(b) In accordance with DoD Instruction 5505.7, unless there is a clear case of mistaken identity, a Federal Court order for expungement, or an error in applying the credible information indexing standard, information contained in the subject or victim block of a report will not be removed from the report or the DCII. Information reflecting a change in the content/context of the ROI will be reflected in the investigative summary of the ROI.

(9) Provide technical guidance to JAs in their capacity as Release of Information Coordinators.

(10) Ensure subjects, suspects, victims, and juveniles are retained in the subject block of a ROI for the USACIDC 40-year retention period.

c. The Chief, FOIA/PA Division will:

(1) Recommend to the Director, USACRC, whether to release information or amend records.

(2) Coordinate requests for access to, or amendment of, records with the staff proponents for the records, USACIDC staff and/or subordinate investigative units, and other agencies as appropriate.

(3) Ensure that all systems of record subject to the PA are described by published system notices, that such systems are not modified or otherwise expanded prior to public notification and that disclosure of personal information and disclosure accounting records are accomplished in accordance with appropriate regulations.

(4) Maintain liaison with the Deputy Chief of Staff for Information Management (DSCIM) and Support (DCSSPT) to ensure that privacy statements are prepared and issued for all forms, formats and questionnaires subject to the PA.

(5) Develop and administer a PA training program for all personnel involved in the design, development, custody, maintenance and use of a system of records subject to the PA.

(6) Maintain narrative and statistical data and prepare required reports concerning release of information and amendments.

(7) Develop policy in coordination with appropriate staff elements for implementation of the FOIA, PA and other release or amendment of USACIDC originated or maintained information.

d. The SJA will:

(1) Implement USACIDC policies and procedures for processing special interest and Congressional inquiries under CIDR 1-20.

(2) Review requests for amendment of criminal investigative records and provide recommendations to the USACRC.

(3) Provide definitive legal advice on FOIA/PA requests.

e. The Office of the Chief of Public Affairs (OCPA) will:

(1) Effect all USACIDC releases of information to media representatives, except those made under the FOIA/PA.

(2) Provide technical advice regarding public affairs implications when requests from media representatives are made under the FOIA.

(3) Coordinate FOIA releases to the media with HQDA and local public affairs offices, when appropriate.

f. The Deputy Chief of Staff for Operations (DCSOPS) will:

(1) Review requests for amendment of criminal investigative records and provides recommendations to the USACRC.

(2) Ensure that policies pertaining to the collection, control, exchange and distribution of personal data and records are in compliance with the PA and pertinent regulations.

g. The DSCIM will:

(1) Provide for training upon request of personnel involved in the design, development, custody, maintenance, scope and use of systems of records covered by the PA.

(2) Review policies relating to the collection, control, distribution and exchange of USACIDC maintained investigative information and records for compliance with the requirements of the PA and other regulations.

(3) Ensure that PA requirements are covered in the design, documentation, and content of present or future USACIDC automated management information systems.

(4) Ensure that policies developed pertaining to the collection, control, exchange and distribution of personal data and records are in compliance with the PA and pertinent regulations.

h. The DCSSPT will:

(1) Coordinate changes to files systems subject to the PA system notice requirements with the USACRC.

(2) Coordinate new and revised forms with the USACRC to ensure that privacy statements are prepared when required.

(3) Act as proponent in the review of requests for access to, or amendment of, accreditation files, and provide the USACRC with recommendations, upon request, whether requests should be granted or denied.

(4) Ensure that policies developed pertaining to the collection, control, exchange and distribution of personal data and records is in compliance with the PA and other regulations.

i. The USACIDC IG will:

(1) Inspect USACIDC implementation of, and compliance with, the FOIA/PA.

(2) Serve as the USACIDC point of contact with the DAIG for release and amendment of USACIDC records contained in IG files and records included in USACIDC files.

j. USACIDC investigative units will:

(1) Ensure that policies developed pertaining to the collection, control, exchange and distribution of personal data and records are in compliance with the PA and other regulations.

(2) Release USACIDC originated records/information or records to requesters when such release is a routine use described in the PA system notice for the record/information requested.

(3) Will not deny requests made under the FOIA/PA. Refer requests for release of information to the Director, USACRC. Refer requests for non-USACIDC originated information to the appropriate agency, if known, or to the Director, USACRC, for action or referral of the request.

(4) Prepare supplement ROIs to affect approved amendments of those reports less than three years old.

(5) Maintain CIDF 118-E-R on disclosures made to persons or agencies outside of DoD and forwards the original CIDF 118-E-R to the USACRC for filing with the final ROI.

(6) Maintain a record of FOIA/PA requests received and disposition made (e. g., referred to the Director, USACRC, referred to other appropriate agency).

(7) Ensure that personnel assigned to their activity receive training on FOIA/PA policies.

25-34
Procedures

a. USACIDC Processing of Requests for Release of Information.

(1) The Director, USACRC, act on those requests for investigative files or information maintained by the USACRC that are requested by any agency for a routine use (law enforcement purpose) or by agencies within the Executive Branch solely for their use. Requests for USACIDC records by an agency within the Executive Branch for subsequent release outside that agency will be referred to the Director, USACRC.

(2) The Chief, OCPA, responds to those requests for information received from the media, except those made under the FOIA/PA. All FOIA/PA requests from the media will be referred to the Director, USACRC, for action. The USACRC will coordinate final release action with OCPA.

(3) The Chief FOIA/PA Division will.

(a) Process all release of information actions that are not specifically designated or authorized to be accomplished by other USACIDC investigative units. The USACRC will obtain records/information requested from the appropriate USACIDC investigative unit at which the information is likely to be maintained.

(b) Coordinate requests for amendment of records with proponents so designated by this chapter, or others, when appropriate.

(c) Effect denials of requests for information by the CG, USACIDC, under the FOIA/PA, as appropriate.

(d) Collect fees from requesters as authorized by AR 25-55 and AR 340-21.

(e) Process or acknowledge individual requests within 20 business days from the date of receipt.

b. USACIDC Investigative Unit Processing of Requests of Information.

(1) Release by Investigative Units. Records/information may be released when such release is a routine function of the respective USACIDC investigative unit and the purpose for which information is to be released is routine.

(2) Referral by Investigative Units. Whenever the receiving investigative unit is not authorized to affect the release, requests for information should be referred to the Director, USACRC. However, if a request is received for non-USACIDC records/information, the request may be referred directly to the custodian of that

records/information without referral to the USACRC. In all instances, the requester must be advised of the referral in writing as soon as possible, but not later than 10 business days after receipt of the request. Requests referred to the Director, USACRC, or other release authority, should be accompanied by:

(a) A copy of all records not on file at USACRC (i.e., local action sequence only files such as a Target Analysis File or Significant Data File) pertinent to the request that are contained in the investigative unit's files.

(b) A statement in the LOT as to whether there are any reasons for withholding the records/information, or portions thereof. The reason(s) for such recommendations must be fully explained and should relate specifically to one or more of the FOIA exemptions.

(c) A copy of the interim reply furnished to the requester.

(3) Coordination of requests for USACIDC records.

(a) Local SJA. Requests for USACIDC records for the purpose of litigation or filing claims against the U.S. Government should be coordinated with the local SJA. Requests from a defense counsel should be coordinated with the trial counsel or civilian prosecutor to determine whether a FOIA exemption should be exercised to withhold records, or portions thereof.

(b) Local IG. Whenever USACIDC originated records have been created in connection with an IG investigation, coordination should be made with that office to determine any interests to be protected.

(c) Local Public Affairs. Requests from media and the public that are anticipated to have high potential for media interest should be coordinated with the local public affairs and/or USACIDC OCPA.

(d) Other Law Enforcement Agencies. When USACIDC originated records pertain to matters within the jurisdiction of other law enforcement agencies, or pertain to on-going investigations, coordination will be effected with the agency concerned.

(4) Disclosure accounting:

(a) A CIDF 118-E-R must be prepared for all releases of information outside the DoD. Accounting should be made for all other disclosures of records, which are not specifically identified in the text of the record, or in the distribution block of the ROI.

(b) A copy of the CIDF 118-E-R will be maintained with the office file from which the information was released. The original CIDF 118-E-R must accompany the final ROI forwarded to the USACRC or filed at another location.

(5) Time limits. The receiving investigative unit will acknowledge receipt of a request, in writing to the requester and effect release or referral, as appropriate, within 10 business days.

c. USACRC FOIA/PA Request for Records Maintained by USACIDC Investigative Units

(1) Time Limits. The FOIA and PA each impose statutory time limits for processing requests, as do the DoD and Army implementing regulations. The FOIA imposes a 20 business day period, and the PA imposes a 30 calendar day period. These time periods begin upon receipt of the FOIA/PA by USACRC and encompass the entire processing time, including gathering responsive records, sanitizing records, and issuing final responses to requesters. These time limits can be extended (minimally) in cases where records are maintained in separate geographical areas. The PA time limit is also applicable to PA amendment requests. USACIDC elements in receipt of a USACRC request for records under the FOIA\PA must complete a search for responsive records and dispatch the results of the search to USACRC within 7 business days.

(2) Required searches for records. A complete and thorough search is required for all records that may be responsive to the request. The request should be interpreted in the broadest possible sense. Even if records appear remotely responsive, they must be provided to the FOIA/PA Division for review and release determination. In support of these required searches for records, USACRC will either forward a copy of the incoming request or provide a paraphrased version to the responsible USACIDC office. The request will be accompanied by a memorandum requesting a search for records to be conducted (figure 25-1). As the Director, USACRC is not the custodian of locally maintained USACIDC records, a generic response memorandum attesting to the thoroughness of the search will also be provided for USACIDC offices to complete upon their conclusion of the records search (figure 25-2).

(3) Required reproduction of records. It is required that complete, readable copies of responsive records and files be provided, including, but not limited to, agent activity summaries**,** exhibits, notes, and related e-mail messages. Providing records to the FOIA/PA Division does not mean the records will be released to the requester. The FOIA/PA Division will make release determinations on a case-by-case basis in accordance with current information release requirements. However, it is important to note that even if records are exempt from disclosure, the documents are still required to be provided to and maintained by the FOIA/PA Division.

d. Processing requests for amendment of USACIDC records.

(1) General Information:

(a) Individuals who believe records pertaining to themselves are inaccurate may request to have those records amended. The burden is on the requester to demonstrate that an amendment is warranted by providing new, relevant material facts that are determined to warrant their inclusion in, or revision of, the record(s) in question.

(b) Records compiled for law enforcement purposes are exempt from amendment. However, this exemption is permissive and should be exercised only when "a significant and legitimate government purpose" is served by not granting the request for amendment.

(c) Generally, requests for amendment of USACIDC records pertain to amendment of ROIs (e. g., removal of name from subject block or changing the probable cause determination of the investigative summary).

(d) Prior to 1 July 1992, an individual or entity was listed as a subject of a ROI (and thus indexed into the DCII) by applying a probable cause standard. If during the course of the investigation, operational review, or the amendment review process it was determined that evidence fell beneath the probable cause standard, the individual or entity was removed from the subject block of the report, the DCII, and placed into the ASCRC. This procedure is still in place for ROIs closed prior to 1 July 1992.

(e) After 14 May 1992, DoD Instruction 5505.7 mandated credible information as the standard for listing a person or entity as the subject of a ROI and indexing in the DCII. A subject was listed in a ROI when it was determined that credible information existed that a person or entity may have committed a criminal offense or was otherwise made the object of a criminal investigation. At the time DoDI defined credible information as:

"Information disclosed or obtained by an investigator, considering the source and nature of information and totality of circumstances, is sufficiently believable to indicate criminal activity has occurred and would cause a reasonable investigator under similar circumstances to pursue further the facts of the case to determine whether a criminal act may have occurred."

The probable cause standard was retained to determine whether the offense reported was founded, unfounded, or insufficient and is documented in the investigative summary of the ROI. Under DoD Instruction 5505.7, once listed in the subject block of a ROI, an individual or entity may be removed from the subject block of the report and the DCII only in instances of mistaken identity or when an error was made in applying the credible information standard (i.e., at the

time of the initial ROI, there was no credible information that the subject had committed an offense), and not during subsequent investigation determines that credible information does not now exist. In addition, the probable cause determination documented in the investigative summary (founded, unfounded or insufficient) may be amended as determined necessary by operational review or during the amendment request process. Evaluation of the probable cause standard is a separate and distinct review performed in addition to evaluation of the credible information standard.

(f) After 7 January 2003, DoD Instruction 5505.7, continued to mandate credible information as the standard for listing a person or entity as the subject of a ROI and indexing in the DCII but the standard was refined and the requirement to list a person who was otherwise made the object of a criminal investigation was eliminated. The current definition of credible information is:

"Information disclosed or obtained by an investigator that, considering the source and nature of information and totality of circumstances, is sufficiently believable to lead a trained investigator to presume that the fact or facts in question are true."

The probable cause standard of the investigative summary remains unchanged as do the subject block removal and review procedures listed in paragraph 25-34b(1)(e) above.

(g) Each request for amendment of records submitted under the PA will be considered on its own merit as to the accuracy, relevancy, timeliness or completeness of the record for USACIDC purposes. In those cases where amendment of criminal investigative records is determined proper, a supplemental message report will be prepared and dispatched by the originating investigative unit or the USACRC, with distribution as appropriate.

(2) Requests Received by USACIDC investigative units:

(a) The receiving investigative unit will acknowledge receipt of the request, in writing, to the requester within 10 business days after receipt of the request. The request, along with the subject record, will be forwarded to the Director, USACRC. The requester will be notified in writing of the referral.

(3) Requests Received by USACRC/HQUSACIDC:

(a) The Director, USACRC will:

1. Serve as the single command point of contact for the receipt, processing and reply to requests for amendment of USACIDC records submitted under the PA.

2. Forward requests for amendment of criminal investigative records to the SJA for legal review, to the DCSOPS for operational review, and appropriate major subordinate command (for cases less than three years from date of closing) for case review, evaluation, and recommendation. Amendment requests for accreditation files will be forwarded to the DCSSPT for review, evaluation, and recommendations.

3. Conduct a thorough case review of criminal investigative records subject to a request for amendment to form an opinion as to whether the request for amendment appears to be proper for approval.

4. Effect staff and field coordination as described below.

5. Impose a 20 business day suspense on all proponents reviewing records in response to requests for amendment. This suspense includes requests reviewed by investigative units. Processing of the request will proceed without the input of any proponent that does not meet the suspense.

6. Determine in each case, after the record proponent accomplishes review, whether there exists a significant and legitimate government interest in not amending the subject record as requested. If the determination is that the record should be amended, effect amendment by supplemental ROI, annotation, deletion, or destruction of the record, whichever method is deemed most appropriate.

7. Notify the requester of the final USACIDC decision on the request.

8. Take action to remove names from the DCII and other indices, as appropriate.

(b) The DCSOPS will:

1. Conduct a thorough case review of criminal investigative records subject to a request for amendment, accomplishing normal staff and/or field coordination and corrective action as deemed appropriate.

2. Provide the USACRC the case review results and a recommendation whether the request for amendment appears proper for approval.

(c) The DCSSPT will:

1. Review requests for amendment of accreditation files, accomplishing corrective action as deemed appropriate.

2. Make recommendations to the USACRC on requests for amendment.

(d) The SJA will:

1. Make recommendations to the USACRC on requests for amendment.

2. Make final determinations on legal issues.

(e) The Commander, USACIDC major subordinate command level will:

1. Conduct a thorough case review of criminal investigative records subject to a request for amendment.

2. Make recommendations to the USACRC on requests for amendment.

3. Ensure timely compliance by subordinate investigative units of administrative requirements associated with amendment requests.

(4) Staff Policy:

(a) In the event that the DCSSPT and the SJA conclude that the request for amendment of accreditation files is proper for approval, the USACRC will notify the requester of this determination.

(b) During the case review process, when the DCSOPS, USACRC, SJA and the USACIDC major subordinate command (for cases within three years of the date of the final ROI) believe that the request for amendment is proper for approval, the USACRC will notify the originating USACIDC investigative unit to prepare a supplemental ROI reflecting the command determination.

(c) In the event there is a disagreement between the reviewing activities on whether the amendment is proper for approval; and which disagreement cannot be resolved, the USACRC will prepare the action for determination by the CG, USACIDC.

(d) When a request for amendment is approved, the amendment will be effected and the requester and all prior recipients of the record will be notified and/or provided a copy of the amended record.

(e) When a request for amendment is denied, the requester will be notified of the final determination and reason(s) for denial.

CHAPTER 26

26-1
Purpose

This chapter sets forth the organization and scope of responsibilities of the U.S. Army Criminal Investigation Laboratory (USACIL). It also prescribes policies and procedures associated with requesting laboratory and technical services and criminalistics support. AR 195-2, Criminal Investigation Activities, Chapter 6, U.S. Army Criminal Investigation Laboratory, and CIDR 10-1, Organization and Functions, Chapter 4, U.S. Army Criminal Investigation Laboratory, also set forth the mission, functional responsibilities and policies of the USACIL.

26-2
Organization and Mission

The USACIL is a major subordinate command within the USACIDC providing forensic laboratory services worldwide to Department of Defense Criminal Investigative Organizations (DCIO) and other federal law enforcement agencies. The USACIL also manages the USACIDC Criminalistics Program.

26-3
Responsibilities

a. Laboratory services.

(1) In support of DCIO interests, the USACIL provides forensic laboratory examinations in at least the following seven disciplines and identifies and coordinates necessary examinations beyond the capabilities of the USACIL:

(a) Trace Evidence.

(b) Drug Chemistry.

(c) Serology/DNA.

(d) Latent Prints.

(e) Questioned Documents.

(f) Imaging and Technical Support (photography, audio/video enhancement, computer-related crime).

(g) Firearms and Toolmarks.

(2) Where the DoD has an investigative interest and there is no legal or administrative prohibition such as Posse Comitatus, the USACIL may respond to requests from state, local, and foreign government agencies. The USACIL's support must be approved by the USACIL Commander (CDR) or the Laboratory Director (DIR).

b. On-site support. For USACIDC, the USACIL also provides on-site crime scene support to help in the processing of crime scenes, and operational support beyond the capability of the requester, such as technical services, computer-related crime and any other forensic consultations as deemed appropriate. Primary mission commitments permitting, these services are also available to other USACIL customers.

c. Research and development.

(1) Laboratory. To ensure a state-of-the-art forensic laboratory capability is maintained, the USACIL conducts research and applications development. The goal is to commit up to ten percent of examiner time to research and development on an annual basis. Every reasonable effort will be made to publish and present research and development results in applicable professional forensic journals and forums, as prescribed in chapter 5 of this regulation.

(2) Criminalistics. The USACIL manages the USACIDC criminalistics program, as defined in Chapter 22, Criminalistics Program, of this regulation. In this regard, the USACIL assists USACIDC in maintaining a state-of-the-art investigative posture by identifying, evaluating and standardizing investigative techniques and equipment; providing training on that equipment and those techniques; responding to operational support requirements beyond the capability of the USACIDC and the USACIL in areas such as technical services, computer-related crime, and any other forensic science consultations as deemed appropriate. The specific responsibilities of the USACIL in these areas are delineated in CIDR 70-1, Evaluation & Acquisition of USACIDC Equipment, and Chapter 22 of this regulation.

d. Expert witness testimony. In accordance with AR 195-2, paragraph 6-4, Court Appearances, USACIL examiners are available to provide expert witness testimony regarding completed forensic examinations.

e. Training. The USACIL provides training in the laboratory and at field locations in the forensic sciences, use and maintenance of field investigative equipment and investigative techniques. This training is provided for investigators, legal personnel and others who may benefit from the information.

26-4
General policy of operation

To assure effective resource management while providing for timely, impartial and quality service in support of criminal investigations within the DoD, the USACIL CDR and DIR will establish policies and procedures associated with the daily operations of the laboratory and criminalistics support provided by the USACIL, to include the processing and control of evidence.

26-5
Procedures for requesting support

a. Laboratory examinations. Investigative and law enforcement agencies supported by the USACIL may submit evidence directly to the laboratory. Prior coordination is encouraged to ensure the laboratory is capable of providing the desired service. Other activities should submit evidence through their supporting DCIO or other law enforcement agency. If forensic laboratory examinations within the capability of the USACIL are desired from other than the USACIL, prior approval must be obtained from the USACIL CDR or DIR. The USACIL does not examine evidence in support of administrative actions/inquiries without the prior approval of the USACIL CDR or DIR. The USACIL address is as follows:

MAILING ADDRESS:

Laboratory Director
U.S. Army Criminal Investigation Laboratory
4553 N 2nd
Forest Park, GA 30297-5122

EMAIL ADDRESS:

mail131@usacil-acirs.army.mil

(1) Priority of examinations. Normally, the USACIL will process requests on a first come, first serve basis, unless expeditious handling is specifically requested and justified. The USACIL CDR and the DIR have the authority to expedite laboratory services. In accordance with AR 195-5, expedites will normally be limited to those situations specified below:

(a) The subject is being held in pre-trial confinement.

(b) A trial date is set.

(c) Results are needed for an Article 32 investigation.

(d) Results are needed for an Article 39a session.

(e) The subject is due to transfer, separate, or reenlist.

(f) Investigator assigned to the case is scheduled for permanent change of station (PCS) or expiration of term of service (ETS).

(g) The analysis of covertly acquired controlled substances is needed for further investigation.

(h) The USACIL DIR determines that other valid reasons exist, such as:

1. Death investigations or other serious crimes against persons where a suspect has been identified.

2. Situations involving national security.

3. Monitorship cases as specified in this regulation.

4. Other situations at the discretion of the expedite approval authorities.

(2) Re-examination of evidence. The USACIL will not re-examine evidence previously examined in the same forensic discipline by another laboratory, nor accept evidence which is to be examined by another laboratory in the same forensic discipline, except as follows:

(a) When ordered to do so by a court of competent authority.

(b) The USACIL has more exacting and sophisticated equipment or techniques for the examination, which could significantly improve the reliability of the findings as determined by the USACIL DIR.

(3) Serological testing of urine specimens. The USACIL will only conduct serological analysis of urine specimens received from DCIOs and other law enforcement agencies in the following situations:

(a) The analysis supports an ongoing investigation by the agency.

(b) The analysis has potential for resolving a DoD member's contention that urine identified as his which tested positive for drugs in the DoD Drug Abuse Testing Program was, in fact, not his. However, in this situation, before the analysis will be performed, the member must undergo a polygraph examination where the results are inconclusive or the examiner fails to offer an opinion due to no fault of the member being tested.

(c) The analysis is ordered by a court of competent authority.

(4) Expanding examinations. The USACIL will not necessarily limit examinations to those requested. In the interest of the administration of justice, the USACIL will identify all practicable examinations within its capabilities to provide. Examinations identified by the USACIL as necessary to the administration of justice, but which have not been requested by the submitter, should be coordinated with the submitter.

(5) Suspension/cancellation of examinations. Although the USACIL will normally complete all examinations requested and those additional examinations deemed necessary to the administration of justice, there may be occasions when it would not be in the best interest of the administration of justice nor effective resource management to continue with programmed examinations. When this situation is identified by the submitter, the submitter will notify the USACIL by the most expeditious means. In those cases where the USACIL identifies an examination(s) that would not have probative value, the USACIL will coordinate with the submitter by the most expeditious means available. Upon such notification by either the submitter or the USACIL, the laboratory will suspend the affected examination(s) and return the evidence and laboratory request if all other work has been completed. A report of any actions or findings developed prior to the cancellation request will be published. This report will explain why and at whose request the examination(s) were cancelled/suspended.

(6) Rejection of cases/termination of analysis. The USACIL CDR and DIR have the authority to reject case submissions or specific analysis and to terminate analysis in the following instances:

(a) The USACIL personnel or property would be subjected to unreasonable risk during the evidence examination.

(b) Coordination with the SJA supporting the laboratory indicates the request is unreasonable or unnecessary.

(c) Requested examinations are not within the capability of the USACIL.

(d) In other situations deemed appropriate by the USACIL CDR or DIR. When cases are rejected or analysis terminated by the USACIL, the circumstances will be reported to the requester.

(7) Forensic laboratory services beyond USACIL capabilities. When forensic laboratory services beyond USACIL’s capabilities are needed to support criminal investigations within the DoD, the USACIL will identify appropriate activities that can provide the needed services. In support of USACIDC investigations, the USACIL will also coordinate and pay for the requested services.

(8) Notification required when evidence will be consumed in examination. If requested examinations will result in consumption of evidence to the degree that evidence cannot be re-tested, the laboratory will notify the case agent. The case agent is responsible for offering the defense counsel the opportunity to personally, or by means of an expert obtained by the defense, view the examination and concurrent destruction of the evidence. If there is no defense counsel assigned, the responsible SJA will be notified by the case agent. If there is no response from the defense counsel or SJA, the laboratory will begin examinations seven working days after the information is given to the case agent.

(9) Results of examinations. Results of USACIL examinations will be provided only to the submitter or activities authorized by the submitter. Normally, only final reports will be issued; however, interim reports may be issued, if necessary.

(10) Release of case file materials. The USACIL will not release case file materials such as examiner notes without approval of the trial counsel or the SJA responsible for the case. All requests for documents from a case folder must be coordinated with and approved by the responsible trial counsel or SJA.

(11) Release of ancillary documentation. Examiner training records, personnel records, and other like documentation will not be released without a court order. Examiner curriculum vitae are not maintained by the USACIL and are the sole property of the examiner. The examiner alone decides when it is appropriate to release the curriculum vitae.

(12) Transfer of cases. Transfer of cases to laboratories outside the USACIL system will not be done without the prior approval of the submitter.

b. Crime scene support. A USACIDC request for assistance in processing crime scenes should be directed through the appropriate USACIDC major subordinate CDR to the USACIL DIR. All other agencies should submit requests through their local investigative field unit CDR. The USACIL DIR will evaluate the request and determine the appropriate course of action. The requesting agency will fund crime scene support.

(1) Crime scene support alternatives. Alternatives to the USACIL on-site support include consultation and referral to other resources.

(2) Release of reports. Reports of crime scene support, like laboratory examination results, will be provided only to the submitter and activities authorized by the submitter.

c. Forensic sciences and technical services (criminalistics) support. Normally, these services are only available to USACIDC activities and are covered in Chapter 22 of this regulation. The USACIL CDR and DIR can grant exceptions to

this policy. In all cases, criminalistics support will be funded by the requesting agency.

(1) Identification of requirements. The USACIDC activities needing support in these areas should identify requirements to their supporting USACIDC major subordinate command technical service coordinator or forensic science coordinator, as appropriate. If the needed support is beyond the capability of the USACIDC major subordinate command, the USACIDC major subordinate CDR will identify the requirements and request assistance from the USACIL CDR or DIR, ATTN: CILA-BIT (Imaging & Technical Support Division).

(2) Coordination of requirements. Throughout the validation of need process, coordination between the requester, the USACIDC major subordinate command and the USACIL Imaging & Technical Support Division is encouraged to ensure expediency in operations and effective resource management.

(3) Required reports. An after-action report will be prepared at the completion of all criminalistics support activities and a copy will be forwarded to the requester. If required by the requester, an Agent’s Investigation Report will be prepared for inclusion in the requester's report of investigation and will be provided to the serviced activity upon completion of the service. Any other distribution of such reports will be made only with the approval of the serviced activity.

d. Training support.

(1) The USACIL provides the following training:

(a) Special Agent Laboratory Training (SALT). The SALT is a one-week, on-site course targeted primarily for special agent-in-charge (SACs), Forensic Science Coordinators, and those who can train others. The training is a balance of lectures and hands-on training in collecting, handling and processing physical evidence. Major subordinate commands are responsible for providing names of nominees for attendance. Priority for attendance is given to USACIDC elements; however, slots are offered to other DoD agencies, when available. The training is offered a minimum of four times per year.

(b) On an annual basis, within resource constraints, the USACIL will program and conduct training in the areas of technical services, investigative techniques, computer-related crime, etc., for each of the USACIDC major subordinate commands and other USACIDC elements, as deemed necessary. This training will be scheduled in coordination with the USACIDC major subordinate commands to maximize the training audience and opportunity. The USACIL will budget for and fund annual technical investigative equipment training.

(c) Technical services training for the U.S. Army Military Police School in USACIDC courses. The requestor will fund the training.

(d) Opportunity training associated with court testimony. As USACIL mission requirements allow, USACIL examiner(s) traveling to provide testimony in court cases will offer to provide limited training in their forensic specialty to the agents and SJA personnel at their TDY location.

(e) Support to the DoD Judge Advocate schools for the various forensic disciplines, as requested, and as mission requirements allow. The training will be funded by the requester.

(f) A compilation of forensic articles in the form of a technical bulletin will be published and distributed to DCIOs worldwide for use as a training tool for investigative agents.

(2) Requests for training related to laboratory services and crime scene processing should be submitted in writing to the USACIL DIR. The USACIL DIR will weigh primary mission requirements and available resources in determining whether or not to approve the request. The laboratory will take all reasonable action to honor valid requests or will refer the requester to alternative resources. The requester will fund the training.

e. Expert testimony. Requests for court appearances of USACIL personnel will be processed in accordance with AR 195-2, Criminal Investigation Activities, Chapter 6, U.S. Army Criminal Investigation Laboratory, paragraph 6-4, Court Appearances. Advance notice of ten working days is normally required to ensure administrative requirements are accomplished and availability of personnel. USACIL examiners will not testify against other USACIL examiners or serve as defense consultants unless such activity is approved by the CG, USACIDC.

26-6
Evidence submission requirements

The following guidance is designed to apply to all evidence submitters. DA submitters are further guided by requirements in this regulation, AR 195-5 and FM 19-20, Law Enforcement Investigations. If any submitter has questions or doubts concerning evidence submission, contact the USACIL for guidance.

a. Submission of evidence. Evidence must be submitted under chain of custody and accompanied by a crime laboratory examination request which identifies the evidence submitted, the examination(s) desired and a synopsis of investigative information pertinent to the laboratory services requested. The primary offense code for the investigation being conducted will be annotated on all crime laboratory examination requests submitted to the USACIL. The offense code will

be placed in the contributor case number section of the request immediately following the sequence/ROI number. All DA units should submit evidence in accordance with AR 195-5, Evidence Procedures, Chapter 2, Recording and Accountability of Evidence.

b. A package wrapped for shipment to the laboratory will contain evidence from only one investigation. Each item of evidence within the shipping container should be in its own separate package. Violation of this procedure can result in contamination of evidence and problems in the chain-of-custody.

c. Pack each item in a way that will minimize friction and prevent the item from shifting, breaking, leaking or contacting other evidence. Pack in cotton or soft paper those items that are particularly susceptible to being broken, marred, or damaged. Wrap each item of evidence separately. Label each item to correspond with its entry on the laboratory examination request and pack it securely in a shipping box. Documentary evidence may be placed in an envelope. Seal the box or envelope containing the evidence with tape. Place the submitter's initials or signature across the sealed flap of the envelope or across the paper tape used to seal the box. Cover the initials or signature with transparent tape.

d. Place the original and one copy of laboratory examination request and the chain of custody document in an envelope. Also, if available, include initial/updated summaries of the investigation, crime scene sketches, photographs, and witness/victim statements, as they are often useful to the laboratory examiners. Seal and tape this envelope securely to the box or envelope containing the evidence. Then wrap the box in heavy paper or seal the envelope inside another envelope and address it to the USACIL.

e. The outer wrapping of packages containing potentially hazardous material, such as biologically contaminated evidence and explosive or caustic evidence, should be clearly marked indicating the type of potential hazard enclosed (e.g., "CAUTION: BIOHAZARD"). Prior to shipping potentially hazardous material to the USACIL, the unit shipping the material should coordinate its intention with the laboratory. Any evidence known to be contaminated with an infectious agent (e.g., HIV or hepatitis virus) is subject to the Code of Federal Regulations (CFR) if shipped through U.S. postal mail channels. The CFR requires the evidence be triple-wrapped, sealed and marked with appropriate warning labels. The USACIL should be contacted prior to shipment for further guidance.

f. The way that evidence is transmitted to the laboratory depends on the type of evidence and the urgency of need for the results. Evidence may be hand carried to the laboratory or sent via registered mail. A government carrier may also transport it. Federal laws prohibit transmitting certain types of items through postal channels. If there is any question on mailing, consult the nearest postmaster and/or the laboratory.

g. Chemicals, gases, unexploded bombs, detonators, fuses, blasting caps, and other explosive or inflammable materials cannot be sent by mail. Before these items are forwarded, notify the laboratory that the shipment is planned and the laboratory must acknowledge receipt of notification. In the notification, give details of how the materials are packed. This will reduce the danger involved in unpacking these items at the laboratory.

h. Liquid blood samples (standards from victims and subjects) and all sexual assault kits collected should be submitted in a box separate from that containing the remainder of the evidence from the case. This evidence should be forwarded to the laboratory under a separate registered mail number. Rape kits from the same investigation may be packaged together. Ensure the evidence is packaged and forwarded to the laboratory in accordance with OSHA standards.

i. All non-porous evidence submitted for latent prints should be processed for “super glue” fuming.

j. Under the provisions of Military Rules of Evidence 1003 and 1004, original documents seized as evidence are considered the “best evidence” available. When original documents are not available, usually resulting from their destruction, copies of such documents will be collected and processed under the same restrictions and requirements afforded original document evidence. In particular, such documents will be collected against receipt (DA Form 4137) and processed through the collecting unit’s evidence depository.

k. Normally, after examinations are completed, the USACIL will return all remaining evidence, the laboratory report, and appropriate related materials to the submitter. After favorable coordination with the responsible staff judge advocate (SJA) and the submitter, exceptions to this policy may be granted by the USACIL CDR or DIR.

l. Evidence, the laboratory report, and appropriate related materials will be returned to the submitting agency by registered mail, unless the USACIL DIR authorizes other means.

26-7
Examiner accessions, training and utilization

a. Examiner accession and utilization. Applicants for examiner positions will be processed and certified in accordance with AR 195-3, Acceptance, Accreditation, and Release of United States Army Criminal Investigation Command Personnel, AR 690 series, Chapter 20 of this regulation, and other applicable civilian personnel regulations.

b. The USACIL CDR and DIR will approve and manage the USACIL Examiner Life Cycle Training Program (ELCTP), which is the professional development plan for USACIL forensic examiners. This program establishes the technical training requirements necessary for both certification as a forensic examiner and maintenance of technical proficiency throughout an examiner's career. It ensures that the USACIDC has a cadre of examiners technically and legally qualified to provide state-of-the-art full service forensic examinations in support of DoD investigative interests. The ELCTP is divided into two phases; the certification phase and the sustainment phase.

(1) Examiner Life Cycle Training Program Certification Phase: This phase begins when an applicant is accepted into one of the courses of study administered by the USACIL or is selected or hired for duties requiring certification as an examiner. This phase ends upon completion of the POI and certification as an examiner in accordance with Chapter 3, AR 195-3. The purpose of the Examiner Certification Phase is:

(a) To produce examiners fully capable of conducting state-of-the-art examinations in their forensic discipline.

(b) To produce examiners qualified as experts in their forensic discipline.

(c) To produce examiners qualified for acceptance into and certification by appropriate forensic professional organizations/associations.

(2) Examiner Life Cycle Training Program Sustainment Phase. This is the professional development plan for certified forensic examiners, focused upon developing and sustaining their professional qualifications to ensure that they are proficient and the examinations performed by them are accurate and state-of-the-art. This phase begins upon an examiner's certification and continues as long as the examiner is employed with the USACIL. The goals of this phase are:

(a) To maintain and enhance the USACIL examiners' state-of-the-art proficiency as forensic examiners. This is accomplished by the attendance of the USACIL examiners at courses involving forensic examination techniques; expositions and symposia concerned with newly developed technology; and instrument operator schools for equipment maintained by the USACIL.

(b) To maintain and enhance the USACIL examiners' qualifications as experts in their forensic discipline.

(c) To maintain and enhance the qualifications of USACIL examiners in support of their advancement in professional forensic organizations. This involves the attendance and presentations at professional forensic associations related to a forensic discipline.

(d) To develop a cadre of examiners nationally recognized as leaders in their forensic disciplines.

(e) To develop new forensic applications through research.

(f) To develop managerial and administrative skills necessary to perform supervisory duties for those examiners identified to fill those positions.

26-8
General

To ensure programs, administrative functions and operations are carried out in an efficient and cost effective manner, internal controls will be established in accordance with AR 11-2, Internal Controls Systems.

26-9
Areas of internal control

a. Overall management and operations.

(1) Command inspections. The USACIL will conduct annual quality audits and be subject to Inspector General inspections in accordance with CIDR 1-201, Organization Inspection Program.

(2) Statistics. The USACIL will maintain statistical profiling data using CID Form 49 (Monthly Report of USACIL Activities). Format and instructions for completing this form are contained in the USACIL Standard Operating Procedures (SOP).

b. Quality assurance. The USACIL will operate under a quality assurance program, which includes proficiency testing monitored by the USACIL, standards of quality for each forensic discipline monitored by the chain of command in the laboratory, and a review of customer satisfaction through periodic surveys. Quality control will include both administrative and technical standards and review.

c. Other controls.

(1) Security inspections required. Physical security inspections will be conducted in accordance with AR 190-13, Physical Security.

(2) Inventories required.

(a) Controlled substances inventories will be conducted in accordance with the 21 CFR 1304.11 and 1304.19 and other guidelines as set forth in the USACIL SOP.

(b) Evidence inventories and inspections will be conducted in accordance with guidelines set forth in the USACIL SOP.

(c) Inventories of government property will be conducted in accordance with AR 190-53, Interception of Wire and Oral Communication for Law Enforcement Purposes; AR 710-2, Inventory Management Supply Policy Below the Wholesale Level; DA Pam 710-2-1, Using Unit Supply System (Manual Procedures); CIDR 710-5, Materiel Management System; and the USACIL SOP.

(3) Internal Review Checklist. Internal control checklists will be completed per instructions received from the Office of the Deputy Chief of Staff for Support, HQUSACIDC.

(4) Review and Analysis (R&A) Reports: The R&A reports will be provided per instructions received from the Office of the Deputy Chief of Staff for Operations, HQUSACIDC.

CHAPTER 27

27-1
Purpose

This chapter prescribes policies and procedures governing:

a. The acquisition and retention of criminal investigative information relating to persons, activities, or organizations not affiliated with DoD.

b. The USACIDC review of criminal investigative records and reporting of suspected violations of policy concerning the acquisition and retention of such information.

c. The USACIDC accomplishment of annual verification requirements UP AR 380-13.

d. The acquisition and retention of other sensitive information.

27-2
Applicability

This regulation is applicable to all personnel assigned to the USACIDC.

27-3
Policy

a. Authorized access to information or evidence acquired pursuant to USACIDC investigative activity is regulated by rules of conduct found in, but not limited to the Uniform Code of Military Justice, AR 27-10, AR 190-22, AR 190-45, AR 195-2, AR 195-5, AR 195-6, AR 25-55, AR 340-21, AR 380-13, AR 600-37 and DA Circular 310-65.

b. Non-DoD affiliation.

(1) The AR 380-13 outlines restrictions on the acquisition and retention of information pertaining to non-DoD affiliated persons or organizations.

(2) However, there are no restrictions imposed by AR 380-13 on information acquired or retained in connection with authorized criminal investigations and law enforcement gathering activities which are not "counterintelligence" related. Accordingly, USACIDC may acquire and maintain information concerning non-DoD affiliated persons or organizations as long as the information acquired or maintained is in connection with authorized USACIDC investigative activity.

c. Other sensitive/prohibited information. The acquisition and retention of certain other categories of information requires continuing command attention and internal review to preclude inadvertent violation of current Army regulations or USACIDC policy:

(1) Prohibited information.

(a) No information will be acquired about a person or organization solely because of lawful advocacy of measures in opposition to U.S. Government policy, or because of activity in support of racial or civil rights interests (AR 380-13).

(b) No record describing how an individual exercises rights guaranteed by the First Amendment will be maintained unless expressly authorized by Federal statute, by the subject individual, or unless pertinent to and within the scope of an authorized law enforcement activity. Exercise of these rights includes, but is not limited to, religious and political beliefs, freedom of speech and the press, and the right of assembly and to petition.

(2) Sensitive information.

(a) Information pertaining to Wiretap, Investigative Monitoring, and Eavesdrop Activities (WIMEA) will be safeguarded and reported as provided in DA Circular 310- 65.

(b) Information pertaining to polygraph examinations and exhibits will be safeguarded and reported as provided in this regulation and AR 195-6.

27-4
General

a. All USACIDC personnel are prohibited from acquiring, retaining, reporting or processing information on persons or organizations not affiliated with DoD, except as required pursuant to authorized USACIDC investigative activities. Such activities include criminal investigations, crime prevention surveys, protective service missions, and the criminal intelligence program.

b. Before acquiring information on persons and organizations not affiliated with DoD, pursuant to normal USACIDC investigative activities, maximum reliance will be placed in acquiring the desired information through liaison at the federal, state and local levels with domestic civil law enforcement and investigative agencies and with foreign host country civil and military officials.

c. Information pertaining to persons and organizations not affiliated with DoD and not required in connection with an authorized USACIDC investigative activity may be inadvertently acquired by USACIDC personnel through various means.

(1) Walk-in sources volunteering information where there is no apparent military interest will be referred, if possible, to the appropriate federal, state, local or foreign law enforcement agency. If the source refuses to consent to such referral and there is an indication of imminent threat to life or property or there appears to be some validity to the information, as much of the information as available will be acquired and immediately disseminated to the proper civilian law enforcement office. If a pledge of confidentiality is requested, the identity of the source will be protected insofar as authorized by law. A CID Form 66 (CID Action Record) will be prepared reflecting that information pertaining to another law enforcement agency's area of investigative responsibility was acquired and reported to that agency. Details of the receipt, to include the identity of the source, the general nature of information acquired and reported, and the person or agency contacted, will be made a matter of record. In the event that referral requires passage through USACIDC channels, a ROI or CIR will not be used. The information will be handled and safeguarded similar to procedures required for criminal intelligence, but the de tailed information will not be included in USACIDC criminal information data banks. After referral of this information, the action will be closed on the CID Form 66 as local information, subject to disposition as provided for other closed CID Form 66 actions. The following sentence will be placed in the synopsis block of the CID Form 66, "This action is retained for system control and Privacy Act purposes in accordance with CID Regulation 195-1, chapter 23."

(2) Information not pertinent to authorized USACIDC activities received from anonymous telephone callers, unsolicited letters and other similar sources will be referred or processed as indicated in paragraph 23-4c(1), above.

(3) Periodicals, pamphlets, offender listings, notes of joint law enforcement meetings and other written materials obtained from civilian police agencies or other sources will be routinely reviewed upon receipt. Information pertinent to authorized USACIDC activities will be recorded and retained in the appropriate functional file (e.g., criminal information file). Personal information not pertinent to authorized activities will not be recorded. Preprinted documents containing in formation pertinent to authorized USACIDC activities may be retained intact.

(4) Information not pertinent to authorized USACIDC activities will not be solicited, acquired or retained. Positive action will be taken to preclude the dissemination in writing or acquisition of non-affiliated DoD information not related to USACIDC investigative activity except as authorized above.

27-5
Verification

a. Within USACIDC, two procedures exist which verify that prohibited information is not acquired or retained by USACIDC elements:

(1) Routine verifications which are accomplished before information is added to USACIDC records holdings, (e.g., the review of ROIs and investigative information by the USACIDC unit supervisory and command personnel). The information in such holdings does not require further verification by the unit commander/SAC.

(2) Special verifications. Each USACIDC unit commander/SAC must identify each record holding within the unit to which information is added without routine verification. The unit commander/SAC must accomplish a special verification of these holdings periodically, but at least annually. This verification will consist of a physical review of the information in the holding to ensure that prohibited information is not included.

b. Unit record holdings periodically receive other reviews by external agencies or other USACIDC internal review mechanisms such as those conducted by the Department of the Army Inspector General (DAIG) inspections, USACIDC case/report quality reviews, and USACIDC IG inspections. Results of such reviews, when provided the custodian of these records, are appropriate for verification consideration (i.e., records so reviewed during these other reviews may be credited as a routine or special review).

c. These verification procedures apply to investigative files maintained at headquarters level and include action officer information acquisition and retention.

d. All investigative file holdings, with the exception of a CIR, are accessioned ultimately at the Crime Records Center (CRC). An additional verification review of case files is conducted upon accession into CRC. On those few occasions in which information is generated at CRC, that information is subject to the verification, guidance and procedures set forth in paragraphs 25-5b and c of this regulation.

27-6
Report of prohibited information

a. Whenever, either through routine or special verification procedures, a unit commander/SAC or staff supervisor becomes aware of suspected prohibited information in any of the records holdings, that person will bring the matter to the

attention of the next higher commander or the immediate staff supervisor for appropriate disposition instructions.

b. In those cases where the next higher commander or staff supervisor determines that the information is not prohibited a written notification to this effect will be provided to the subordinate element for annotation in the questioned record.

c. In those cases where the next higher commander, staff supervisor or other intermediate command determines that the information is prohibited, the matter will be expeditiously reported through channels to Commander, USACIDC, ATTN: CIOP-CO.

d. In those cases where the next higher commander, staff officer or other intermediate commander cannot determine whether the information is prohibited (i.e., a violation of this regulation), further inquiry through command channels will be made. Referrals by elements immediately subordinate to Headquarters, USACIDC will be forwarded to Commander, USACIDC, ATTN: CIOP-COP-CO.

e. For AR 380-13 (Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organization) purposes and AR 340-21 (The Army Privacy Program), the initial destruction, purging or amendment of investigative record authority is the Deputy Commander (DCO), HQUSACIDC. In no instance will personnel subordinate to the DCO direct destruction or amendment (e.g., deletions) of USACIDC investigative records for suspected AR 380-13 violations.

27-7
Consolidated report of inspection, Report Control Symbol (RCS) DD-A(A)-1118

a. Under the provision of AR 380-13, USACIDC must submit an annual Consolidated Report of Inspections, RCS DD-A(A)-1118, to HQDA not later than 7 August annually. To complete this requirement, all unit commanders/SACs, USACIDC major subordinate commanders and heads of HQUSACIDC staff elements will submit the following information through channels to Commander, USACIDC, ATTN: CIOP-COP-CO:

(1) All information added to records holding of "unit" during the period 1 October 20 _ (previous year) through 30 September 20 _ (current year) has been routinely or specifically reviewed to ensure that no prohibited information is being maintained;

(2) No prohibited information was found; or

(3) Suspected prohibited information was found and appropriate disposition instructions for this information have been requested.

b. Within the USACIDC major subordinate command and subordinate units, these reports must be submitted to the appropriate USACIDC major subordinate command not later than 12 July annually. Each USACIDC major subordinate command will consolidate all subordinate responses and forward them together with a report for the holdings in the USACIDC subordinate command to HQUSACIDC not later than 20 July annually.

27-8
Responsibilities

a. All USACIDC commanders, agents-in-charge and heads of staff elements and separate staff offices at HQUSACIDC and USACIDC major subordinate commands will:

(1) Ensure that criminal investigative information in all files and indexes under their control is retained in accordance with this regulation.

(2) Maintain a copy of this regulation, AR 380-13 and DoD Directive 5200.27, at each USACIDC field or headquarters element in a policy book, and ensure that all investigative and supervisory personnel in that element review the cited regulations at least biannually. A record will be maintained in the policy book reflecting each individual's review and date thereof.

(3) Upon notification of a pending inspection by the Department of the Army Inspector General for compliance with DoD Directive 5200.27 and/or AR 380-13, the commander or SAC will so notify the Commander, USACIDC, ATTN: CIOP-CO, 6010 6th Street, Fort Belvoir, VA 22060, through channels, by telephone or the most expeditious means available. After each such inspection, the results will be immediately reported through channels to HQUSACIDC.

(4) Ensure that verification procedures are accomplished, and that reports of retained prohibited information and annual reports verification are submitted in a timely manner.

b. All USACIDC major subordinate command, district and field office commanders will ensure that each subordinate element is annually inspected for familiarization and compliance with this chapter and AR 380-13.

c. The DCSOPS, HQUSACIDC, will:

(1) Exercise principle staff responsibility for the doctrinal development of policies and procedures concerning USACIDC acquisition, retention, reporting, and verification of criminal investigative information.

(2) Serve as the headquarters staff focal point for all doctrinal coordination on the acquisition or retention of information regarding non-DoD affiliation and other matters of DIRC interest affecting USACIDC.

d. The Office of the Deputy Chief of Staff for Operations, HQUSACIDC, will:

(1) Exercise principle staff responsibility for the supervision of subordinate implementation of policies and procedures pertaining to verification of USACIDC acquisition and reporting of criminal investigative information.

(2) Serve as the staff focal point for all operational coordination on non-DoD affiliation, acquisition or retention matters affecting USACIDC to include, but not limited to:

(a) Conducting special operational reviews of suspected prohibited information as submitted by subordinate elements in accordance with paragraph 23-5d, this regulation.

(b) In the event of a determination by HQUSACIDC that a violation of AR 380-13 has occurred, reporting apparent violations of AR 380-13 to HQDA (DAMI-PO), Washington, DC 20310, to include circumstances of discovery and corrective action taken.

(c) In the event that USACIDC elements are inspected by the DAIG for compliance with DoD Directive 5200.27 and AR 380-13, notifying HQDA (DAMI-PO), Washington, DC 20310.

(d) Consolidating annual verification reports from subordinate elements, HQUSACIDC staff elements to include CRC, and preparing a written report for submission to HQDA (DAMI-PO), Washington, DC 20310. This letter report will b e approved and submitted by 7 August annually and will reflect report of annual inspection and verification results for compliance with AR 380-13.

e. The Staff Judge Advocate, USACIDC, will provide legal advice and guidance in matters pertaining to the acquisition, retention, dissemination and amendment of investigative records containing information on persons and organizations not affiliated with the DoD.

f. The Inspector General, USACIDC, will inspect all elements of the command to determine compliance with this regulation in accordance with CID Regulation 20-1.

APPENDIXES

A. Criminal Offense Codes
B. Major Command Assignment Codes (MCAC)
C. Hypnosis Policy
D. Criminal Investigation Standards
E. Liaison Program
F. Cooperation with Civilian Law Enforcement Officials (CLEO) Reports
G. DoD Hotline Program
H. U.S. Army Audit Agency
I. Defense Contract Audit Agency
J. Presentations to Prosecutors
K. Subpoena Documentation
L. Suggested Guide for Preparing a MOU for Drug Suppression Operations
M. A Guide to Source Handling
N. Control Room Standard Operating Procedures
O. Preparation of FD Form 249 and FBI/DOJ Form R-84 (Final Disposition Report)
P. Daytime Practical Pistol Qualification Course
Q. Nighttime Practical Pistol Sustainment Course
R. Range Operations and Safety
S. Internal and External Sources
T. Crime Analysis
U. Reference Publications

Appendix A
Criminal Offense Codes

A-1. Offense codes. The terminal digits of the CID report of investigation number are the offense code data elements. This portion of the report number is assigned to all types of CID reports of investigation, criminal intelligence reports, and crime survey reports at the time the report is prepared at the USACIDC unit.

a. Single offense. In cases involving a single offense, the offense code could be as few as two digits, but usually will be three or more digits to depict more accurately the specific elements of the act being investigated.

b. Multiple offenses. Where cases involve multiple offenses or other special circumstances, the multiple digit offense codes which most accurately depict the facts of the act being investigated will be used. This listing will begin with the code for the most serious offense followed by the codes for all other offenses.

A-2. Primary offense code. Seriousness of the offense codes will be based on the maximum punishment listed in the UCMJ, the Federal Criminal Code, or the applicable local statutes or criminal codes applicable to the matter under investigation. The fact that an allegation may later become unfounded will not affect determination of the primary offense code.

a. Same seriousness. When the maximum punishment is the same for more than one offense, the codes for these offenses will be listed in chronological order.

b. Exceptions. Offense codes 5V, 5W, and 5Y, when used will always be the last offense codes listed, immediately preceding the 9 series of offense codes. The 9 series offense codes will always be the last code(s) listed.

A-3. Detailed offense code. The basic offense categories are further distinguished by the detailed offense code additions presented below. The detailed offense code is a combination of numerals and letters used to further breakdown specific listings to key elements of the incident. The detailed offense code will consist of a maximum of five alternating alpha numeric characters as follows:

a. 1st character - numeric designator to identify basic crime category as outlined here:

5 - Crimes against the person.
6 - Sex crimes.
7 - Crimes against property.

8 - Fraud crimes.
9 - Special investigative activities.

b. 2d character - alphabetic listing to reflect a breakdown of sub-categories of offenses under the basic crime category identified. Single capital letters are used for this purpose. NOTE: the letters "I" and "O" are not used to prevent confusion with numeric listings. EXAMPLE: 5N, the "5" identifies the basic category as crime against the person and the "N" identifies the sub-category as the specific offense of "robbery".

c. 3d character - numeric listing to further breakdown the sub-category of the basic crime category listed. EXAMPLE: 5N3 -"5" is the basic category, "N" the sub-category for "robbery" and the "3" further identifies the offenses as "robbery of a business".

d. 4th character - alphabetic listing to provide more detailed breakdown of the incident. EXAMPLE: 5N3A - this fourth character "A" clearly shows the robbery of the business was accomplished by using a handgun.

e. 5th character - when necessary, is a numeral to continue with a more descriptive breakdown of the incident. EXAMPLE: 5N3A2 - the fifth character "2" now tells us that the robbery of the business as accomplished by two or more individuals using a handgun.

A-4. Special considerations.

a. When using the detailed list of offense codes, begin with the basic category number and work down the page to the appropriate sub-category, down to the third, fourth, and fifth characters when applicable or necessary.

b. The offense codes identifying "by use of computer" means that this code , in its entirety, is not used alone but as a supplemental code to the other applicable offense codes in that same category. EXAMPLE: See 8C Dependency Assistance. If the case involves a fraud of dependency assistance, the code 8C1 is used, however, if the fraud was accomplished by using a computer to perpetrate the offense, then both the code 8C1 and 8C2 would be used and reflected as 8C1/8C2.

c. The offense codes (5D series) identifying domestic (family) violence will be utilized as applicable. Offenses involving situations/individuals not specifically addressed within the offense codes will be documented by customization of the 5D9, Other Family Abuse offense code, to reflect their status.
Example: 5D9, Other Family Abuse - Guardian

A-5. Detailed offense code list. The complete listing of offense codes for use is listed below:

|5 |[CRIMES AGAINST PERSONS]
|5A |[ADULTERY, UNLAWFUL FORNICATION & COHABITATION]
|5A1 |ADULTERY (U134)
|5A2 |UNLAWFUL FORNICATION (U134)
|5A3 |UNLAWFUL COHABITATION (U134)
|5A4 |FRATERNIZATION
|5A5 |PANDERING
|5A6 |PROSTITUTION
|5B |[BIGAMY]
|5B1 |BIGAMY INVOLVING MULTIPLE HUSBANDS
|5B2 |BIGAMY INVOLVING MULTIPLE WIVES
|5C |[ASSAULTS (OTHER THAN SEXUAL)]
|5C1 |[AGGRAVATED ASSAULT]
|5C1A |AGGRAVATED ASSAULT USING HANDGUN
|5C1A1 |AGGRAVATED ASSAULT USING CROSSBOW PISTOL
|5C1B |AGGRAVATED ASSAULT USING A SHOULDER WEAPON
|5C1B |AGGRAVATED ASSAULT USING A SHOULDER WEAPON
|5C1C |AGGRAVATED ASSAULT BY CUTTING OR STABBING
|5C1D |AGGRAVATED ASSAULT USING CLUB OR BLUDGEON
|5C1E |AGGRAVATED ASSAULT USING GLASS BOTTLES, ETC
|5C1F |AGG ASSAULT USING METAL TOOLS, TIRE IRONS, ETC
|5C1G |AGGRAVATED ASSAULT USING CHAINS
|5C1H |AGG ASSAULT USING BRASS KNUCKLES, BLACKJACKS, ETC
|5C1J |AGGRAVATED ASSAULT BY KICKING
|5C1K |AGGRAVATED ASSAULT WITH A BOXER'S FIST
|5C1L |AGG ASSAULT (MULTIPLE INDIVIDUALS STRIKING VICTIM)
|5C1M |AGGRAVATED ASSAULT USING USE OF EXPLOSIVE DEVICES
|5C1N |OTHER AGGRAVATED ASSAULT WITH GRIEVOUS BODILY HARM
|5C1P |AGGRAVATED ASSAULT WITH A VEHICLE
|5C1Q1 |AGGRAVATED ASSAULT: HARM INTENDED, FIREARM
|5C1Q2 |AGGRAVATED ASSAULT: HARM INTENDED, OTHER
|5C1R1 |AGGRAVATED ASSAULT: HARM INFLICTED, FIREARM
|5C1R2 |AGGRAVATED ASSAULT: HARM INFLICTED, OTHER
|5C1S |MAIMING
|5C2 |[SIMPLE ASSAULT]
|5C2A |THREATS
|5C2B |CONSUMMATED WITH A BATTERY
|5C2C |ASSAULT: CHILD UNDER 16
|5C2D |[SPECIAL ASSAULTS]
|5C2D1 |ASSAULT: COMMISSIONED OFFICER
5C2D2 |ASSAULT: WARRANT OFFICER

|5C2D3 |ASSAULT: OTHER NCO/PO
|5C2D4 |ASSAULT: MIL/CIV LAW ENFORCER
|5C2E |[MILITARY ASSAULTS]
|5Y2E1 |ASSAULT: OFFICER EXECUTING DUTY
|5Y2E2 |ASSAULT: IN TIME OF WAR
|5Y2E3 ASSAULT: WARRANT OFFICER
|5Y2E4 |ASSAULT: SUPERIOR NCO/PO
|5Y2E5 |ASSAULT: OTHER NCO/PO
|5D |[FAMILY VIOLENCE]
|5D1 |CHILD NEGLECT
|5D2 |CHILD MALTREATMENT OR MISTREATMENT
|5D6 |[SPOUSE ABUSE]
|5D6A |SPOUSE ABUSE, CIVILIAN FEMALE VICTIM
|5D6A |SPOUSE ABUSE, CIVILIAN FEMALE VICTIM
|5D6B |SPOUSE ABUSE, MILITARY FEMALE VICTIM
|5D6C |SPOUSE ABUSE, CIVILIAN MALE VICTIM
|5D6D |SPOUSE ABUSE, MILITARY MALE VICTIM
|5D7 |[FAMILY MEMBER ABUSE]
|5D7A |[FAMILY ABUSE - CHILDREN]
|5D7A1 |CHILD ABUSE – DAUGHTER
|5D7A2 |CHILD ABUSE - STEP-DAUGHTER
|5D7A3 |CHILD ABUSE – SON
|5D7A4 |CHILD ABUSE - STEP-SON
|5D7B |[FAMILY ABUSE - GRANDCHILDREN]
|5D7B1 |CHILD ABUSE - GRANDDAUGHTER
|5D7B2 |CHILD ABUSE – GRANDSON
|5D7C |FAMILY ABUSE – PARENTS
|5D7D |FAMILY ABUSE – GRANDPARENTS
|5D9 |OTHER FAMILY ABUSE
|5E |CIVIL RIGHTS
|5F |[EXTORTION]
|5F1 |EXTORTION BY BLACKMAIL
|5F2 |EXTORTION BY COERCION
|5G |[FORGERY]
|5G |[FORGERY]
|5G1 |[FORGERY OF NEGOTIABLE INSTRUMENTS]
|5G1A |FORGERY OF A PERSONAL CHECK
|5G1B |FORGERY OF GOVT CHECK (NOT PROCRMT/PROP, COMM)
|5G1C |FORGERY OF COMMERCIAL CHECK
|5G1D |FORGERY OF NONAPPROPRIATED FUND CHECK
|5G1E |FORGERY OF CASHIER'S CHECK
|5G1F |FORGERY OF TRAVELER'S CHECK
|5G1G |FORGERY OF MONEY ORDER
|5G1H |FORGERY OF SAVINGS BOND
|5G1J |FORGERY OF A SECURITY
|5G1K |FORGERY OF WITHDRAWAL FORMS

|5G1L |FORGERY OF GOVERNMENT PROCUREMENT CHECK
|5G1M |FORGERY OF GOVERNMENT PROPERTY DISPOSAL CHECK
|5G1N |FORGERY OF GOVERNMENT COMMISSARY CHECK
|5G2 |[FORGERY OF DOCUMENTS]
|5G2A |FORGERY OF MILITARY IDENTIFICATION
|5G2B |FORGERY OF MILITARY ORDERS
|5G2C |FORGERY OF POST EXCHANGE RATION CARDS
|5G2D |FORGERY OF PROPERTY RECEIPTS/SALES INVOICES
|5G2E |FORGERY OF PROPERTY RECORDS
|5G2E |FORGERY OF PROPERTY RECORDS
|5G2F |FORGERY OF TEST SCORE RESULTS
|5G2G |FORGERY OF CORRESPONDENCE
|5G2H |FORGERY OF LEAVE & PASS DOCUMENTS
|5G2J |FORGERY OF FINANCE OR FISCAL DOCUMENTS (.0015 ETC)
|5G2K |FORGERY OF PAY & ALLOWANCE DOCMENTS (EXCL CHECKS)
|5G2L |FORGERY OF COMMISSARY DOCUMENTS (EXCLUDING CHECKS)
|5G2M |FORGERY OF PROCUREMENT DOCUMENTS (EXCL CHECKS)
|5G2N |FORGERY OF PROPERTY DISPOSAL DOCUMENTS (EXCL CKS)
|5G2X |OTHER FORGERIES (NOT 5G2A - 5G2N) (EXCL CHECKS)
|5H |[HOMICIDE]
|5H1 |[MURDER]
|5H1A |MURDER BY SHOOTING
|5H1B |MURDER BY CUTTING, STABBING OR MUTILATION
|5H1C |MURDER BY STRANGULATION
|5H1D |MURDER BY BLUDGEONING
|5H1E |MURDER BY HANGING
|5H1F |MURDER BY POISONING
|5H1G |MURDER BY GRENADES
|5H1H |MURDER INVOLVING EXPLOSIVES (EXCLUDING GRENADES)
|5H1J |MURDER INVOLVING NARCOTICS OR DANGEROUS DRUGS
|5H1J |MURDER INVOLVING NARCOTICS OR DANGEROUS DRUGS
|5H1K |MURDER INVOLVING ARSON
|5H1L |MURDER BY DROWNING
|5H1M |MURDER BY SUFFOCATION OR ASPHYXIATION
|5H1N |MURDER BY TRAFFIC
|5H1P |MURDER BY OTHER MEANS
|5H1Q |MURDER: PREMEDITATED
|5H1R |MURDER: INTENT TO KILL/INFLICT GREAT BODILY HARM
|5HIS |MURDER: ACT DANGEROUS TO OTHERS
|5H1T |MURDER: WITH SPECIFIED OFFENSE
|5H1U |ASSAULT: WITH INTENT TO MURDER
|5H2 |[VOLUNTARY MANSLAUGHTER]

|5H2A |VOLUNTARY MANSLAUGHTER BY SHOOTING
|5H2B |VOL MANSLAUGHTER - CUTTING, STABBING OR MUTILATION
|5H2C |VOLUNTARY MANSLAUGHTER BY STRANGULATION
|5H2D |VOLUNTARY MANSLAUGHTER BY BLUDGEONING
|5H2E |VOLUNTARY MANSLAUGHTER BY HANGING
|5H2F |VOLUNTARY MANSLAUGHTER BY POISONING
|5H2G |VOLUNTARY MANSLAUGHTER BY GRENADES
|5H2H |VOL MANSLAUGHTER BY EXPLOSIVES (EXCL GRENADES)
|5H2J |VOL MANSLAUGHTER INVOLVING NARCOTICS & DANG DRUGS
|5H2K |VOLUNTARY MANSLAUGHTER BY ARSON
|5H2L |VOLUNTARY MANSLAUGHTER BY DROWNING
|5H2M |VOL MANSLAUGHTER BY SUFFOCATION OR ASPHYXIATION
|5H2N |VOLUNTARY MANSLAUGHTER BY TRAFFIC
|5H2P |VOLUNTARY MANSLAUGHTER BY OTHER MEANS
|5H2P |VOLUNTARY MANSLAUGHTER BY OTHER MEANS
|5H2Q |VOLUNTARY MANSLAUGHTER BY LETHAL INJECTION
|5H1R1 |VOLUNTARY MANSLAUGHTER
|5H1R2 |ASSAULT: WITH INTENT TO MANSLAUGHTER
|5H3 |[INVOLUNTARY MANSLAUGHTER]
|5H3A |INVOLUNTARY MANSLAUGHTER BY SHOOTING
|5H3B |INVOLUNTARY MANSLAUGHTER BY CUTTING OR STABBING
|5H3C |INVOLUNTARY MANSLAUGHTER BY STRANGULATION
|5H3D |INVOLUNTARY MANSLAUGHTER BY BLUDGEONING
|5H3E |INVOLUNTARY MANSLAUGHTER BY HANGING
|5H3F |INVOLUNTARY MANSLAUGHTER BY POISONING
|5H3G |INVOLUNTARY MANSLAUGHTER BY GRENADES
|5H3H |INVOL MANSLAUGHTER BY EXPLOSIVES (EXCL GRENADES)
|5H3J |INVOL MANSLAUGHTER BY NARCOTICS OR DANGEROUS DRUGS
|5H3K |INVOLUNTARY MANSLAUGHTER INVOLVING ARSON
|5H3L |INVOLUNTARY MANSLAUGHTER BY DROWNING
|5H3M |INVOL MANSLAUGHTER BY SUFFOCATION OR ASPHYXIATION
|5H3N |INVOLUNTARY MANSLAUGHTER BY TRAFFIC
|5H3P |INVOLUNTARY MANSLAUGHTER BY OTHER MEANS
|5H3Q1 |INVOLUNTARY MANSLAUGHTER
|5H3Q2 |INVOLUNTARY MANSLAUGHTER, WITH SPECIFIED OFFENSE
|5H4 |[NEGLIGENT HOMICIDE]
|5H4A |NEGLIGENT HOMICIDE BY SHOOTING
|5H4B |NEGLIGENT HOMICIDE BY CUTTING OR STABBING
|5H4C |NEGLIGENT HOMICIDE BY POISONING
|5H4C |NEGLIGENT HOMICIDE BY POISONING
|5H4D |NEGLIGENT HOMICIDE BY GRENADES
|5H4E |NEGLIGENT HOMICIDE BY EXPLOSIVES (EXCL GRENADES)

|5H4F |NEGLIGENT HOMICIDE BY NARCOTICS OR DANGEROUS DRUGS
|5H4G |NEGLIGENT HOMICIDE INVOLVING ARSON
|5H4H |NEGLIGENT HOMICIDE INVOLVING DROWNING
|5H4J |NEGLIGENT HOMICIDE BY SUFFOCATION OR ASPHYXIATION
|5H5 |NEGLIGENT HOMICIDE (TRAFFIC)
|5H6 |OTHER HOMICIDE (JUSTIFIABLE, EXCUSABLE)
|5H7 |ATTEMPTED MURDER
|5H8 |ACCIDENTAL DEATH (OTHER THAN TRAFFIC)
|5H9 |[OTHER DEATHS]
|5H9A |NATURAL DEATH
|5H9B |UNDETERMINED MANNER OF DEATH
|5H9C |[MOBILIZATION/DEPLOYMENT DEATH]
|5H9C1 |HOSTILE FORCES
|5H9C2 |FRIENDLY FORCES
|5J |[IMPERSONATIONS]
|5J1 |[IMPERSONATING AN OFFICER]
|5J1A |IMPERSONATING A U.S. ARMY OFFICER
|5J1B |IMPERSONATING A U.S. NAVAL OFFICER
|5J1B |IMPERSONATING A U.S. NAVAL OFFICER
|5J1C |IMPERSONATING A U.S. AIR FORCE OFFICER
|5J1D |IMPERSONATING A U.S. MARINE CORPS OFFICER
|5J1E |IMPERSONATING A U.S. COAST GUARD OFFICER
|5J1F |IMPERSONATING A FOREIGN OFFICER
|5J2 |[IMPERSONATING AN NCO]
|5J2A |IMPERSONATING A U.S. NCO
|5J2B |IMPERSONATING A FOREIGN NCO
|5J3 |[IMPERSONATING AN AGENT]
|5J3A |IMPERSONATING A CIVILIAN CRIMINAL INVESTIGATOR
|5J3B |IMPERSONATING A MILITARY CRIMINAL INVESTIGATOR
|5J3C |IMPERSONATING A CIVILIAN INTELLIGENCE INVESTIGATOR
|5J3D |IMPERSONATING A MILITARY INTELLIGENCE INVESTIGATOR
|5J3E |IMPERSONATING A FOREIGN CRIMINAL INVESTIGATOR
|5J3F |IMPERSONATING A FOREIGN INTELLIGENCE AGENT
|5J3G |IMPERSONATING A CIVILIAN POLICE OFFICER
|5J3H |IMPERSONATING A MEMBER OF THE MILITARY POLICE
|5J4 |[UNAUTH WEAR OF MILITARY UNIFORM, INSIGNIA, ETC]
|5J4A |WEAR OF MIL UNIFORM, ETC TO IMPERSONATE A SOLDIER
|5J4B |UNAUTH WEAR OF MIL UNIFORM, ETC TO COMMIT FRAUD
|5J4C |WEAR OF MIL UNIFORM, ETC FOR CONFIDENCE GAMES
|5J4C |WEAR OF MIL UNIFORM, ETC FOR CONFIDENCE GAMES
|5J4D |WEAR OF MIL UNIFORM, ETC TO GAIN UNLAWFUL ENTRY
|5J4E |WEAR OF MIL UNIFORM, ETC FELONY (OTR THAN 5J4A-D)
|5J5 |WEARING UNAUTHORIZED INSIGNIA

|5J6 |[IMPERSONATE]
|5J6A |IMPERSONATE, INTENT TO DEFRAUD: OFF, WO, NCO
|5J6B |IMPERSONATE, NO INTENT TO DEFRAUD: OFF, WO, NCO
|5J6C |IMPERSONATE, INTENT TO DEFRAUD: OTHER
|5J6D |IMPERSONATE, NO INTENT TO DEFRAUD: OTHER
|5K |[KIDNAPPING]
|5K1 |KIDNAPPING (RANSOM)
|5K2 |KIDNAPPING (HOSTAGE)
|5K3 |KIDNAPPING (OTHER)
|5L |[CONTROLLED SUBSTANCE VIOLATIONS]
|5L1 |[OPIATES]
|5L1A |SMUGGLING OF OPIATES
|5L1B |DISTRIBUTION OF OPIATES
|5L1C |POSSESSION OF OPIATES
|5L1D |[USE OF OPIATES]
15L1D 1|USE OF OPIATES DETERMINED BY URINALYSIS TEST
15L1D 2|USE OF OPIATES DTMD BY OTHER THAN URINALYSIS TEST
15L1E |GROWING OR MANUFACTURING OF OPIATES
15L1E 1|MFG W/INTENT TO DISTRIBUTE OPIATES
15L1F |POSSESSION OF OPIATES WITH INTENT TO DISTRIBUTE
15L1G |INTRODUCE OPIATES
15L1G 1|INTRODUCE W/INTENT TO DISTRIBUTE OPIATES
15L1H |IMPORT AND/OR EXPORT OPIATES
|5L2 |[MARIHUANA]
|5L2A |SMUGGLING OF MARIHUANA
15L2B |DISTRIBUTION OF MARIHUANA
|5L2C |POSSESSION OF MARIHUANA
35L2C 1|POSSESSION OF MARIHUANA, LESS THAN 30 GRAMS
45L2C 2|POSSESSION OF MARIHUANA, 30 GRAMS OR MORE
5L2D | [USE OF MARIHUANA] |
|5L2D1 |USE OF MARIHUANA DETERMINED BY URINALYSIS TEST
|5L2D2 |USE OF MARIHUANA DTMD-OTHER THAN URINALYSIS TEST
35L2D 3|USE OF MARIHUANA DETERMINED BY URINALYSIS, LESS 3
4|5L2D 2|USE OF MARIHUANA DTMD-OTHER THAN URINALYSIS 30 GR
3|5L2D 1|USE OF MARIHUANA DETERMINED BY URINALYSIS, LESS 3
4|5L2D 2|USE OF MARIHUANA DTMD-OTHER THAN URINALYSIS, 30 G
|5L2E |GROWING OR MANUFACTURING OF MARIHUANA
|5L2E |GROWING OR MANUFACTURING OF MARIHUANA, LESS THAN 3
|5L2E |GROWING OR MANUFACTURING OF MARIHUANA, MORE THAN 3
1|5L2F |POSSESSION OF MARIHUANA WITH INTENT TO DISTRIBUTE

|5L2G1 |INTRODUCE LESS THAN 30 GRAMS OF MARIHUANA
|5L2G2 |INTRODUCE MORE 30 GRAMS OR MORE OF MARIHIANA
|5L2G3 |INTRODUCTION W/INTENT TO DISTRIBUTE MARIHUANA
|5L2H |IMPORT AND/OR EXPORT OF MARIHUANA

|5L3 |[DANGEROUS DRUGS (AMPH/BARBITUATES/PCP/ETC)]
|5L3A |SMUGGLING OF DANGEROUS DRUGS
1|DIST RIBUTION OF DANGEROUS DRUGS |A|
1|5L3C |POSSESSION OF DANGEROUS DRUGS
5L3D | [USE OF DANGEROUS DRUGS OF DANGEROUS DRUGS] |
1 |5L3 D1|USE OF DANGEROUS DRUGS DTMD BY URINALYSIS TEST
1|5L3D 2|USE OF DANGEROUS DRUGS DTMD OTHER THAN URINALYSIS
1|5L3E |MANUFACTURING OF DANGEROUS DRUGS
1|5L3E 1|MFG W/INTENT TO DISTRIBUTR DANGEROUS DRUGS
1|5L3F |POSSESS OF DANGEROUS DRUGS W/INTENT TO DISTRIBUTE
1|5L3G |INTRODUCE DANGEROUS DRUGS
1|5L3G 1|INTRODUCE W/INTENT TO DISTRIBUTE DANGEROUS DRUGS
1|5L3H |IMPORT AND/OR EXPORT DANGEROUS DRUGS
|5L4 |[HALLUCINOGENS (LSD, PEYOTE, MESCALINE, ETC)]
|5L4A |SMUGGLING OF HALLUCINOGENS
1|5L4B |DISTRIBUTION OF HALLUCINOGENS
1|5L4C |POSSESSION OF HALLUCINOGENS
|5L4D |[USE OF HALLUCINOGENS]
1|5L4D 1|USE OF HALLUCINOGENS DETERMINED BY URINALYSIS TES
1|5L4D 2|USE OF HALLUCINOGENS DTMD BY OTHER THAN URINALYSI
1|5L4E |GROWING & MANUFACTURING OF HALLUCINOGENS
1|5L4E 1|MFG W/INTENT TO DISTRIBUTR HALLUCINOGENS
1|5L4F |POSSESSION OF HALLUCINOGENS W/INTENT TO DISTRIBUT
1|5L4G |INTRODUCE HALLUCINOGENS
1|5L4G 1|INTRODUCE W/INTENT TO DISTRIBUTE HALLUCINOGENS
1|5L4H |IMPORT AND/OR EXPORT HALLUCINOGENS
|5L5 |[OTHER (SCHEDULE IV OR V)]
|5L5A |SMUGGLING OF OTHER CONTROLLED SUBSTANCE
2|5L5B |DISTRIBUTION OF OTHER CONTROLLED SUBSTANCE
2|5L5C |POSSESSION OF OTHER CONTROLLED SUBSTANCE
|5L5D |[USE OF OTHER CONTROLLED SUBSTANCE]
2|5L5D 1|USE OF CONTROLLED SUBSTANCE DTMD BY URINALYSIS
25L5D2 |USE OF CONTROLLED SUBSTANCE - OTR THAN URINALYSIS
2|5L5E |GROWING/MANUFACTURING OTHER CONTROLLED

	SUBSTANCE
2|5L5E	1|MFG W/INTENT TO DISTRIBUTR OTHER CONTROLLED SUB
2|5L5F	|POSS CONTROLLED SUBSTANCES W/INTENT TO DISTRIBUTE
1|5L5G	|INTRODUCE OTHER CONTROLLED SUBTANCE
1|5L5G	1|INTRODUCE W/INTENT TO DISTRIBUTE OTHER CONTROLLED
1|5L5H	|IMPORT AND/OR EXPORT OTHER CONTROLLED SUBSTANCE
|5L6	|[COCAINE]
|5L6A	|SMUGGLING OF COCAINE
1|5L6B	|DISTRIBUTION OF COCAINE
1|5L6C	|POSSESSION OF COCAINE
|5L6D	|[USE OF COCAINE]
1|5L6D	1|USE OF COCAINE DETERMINED BY URINALYSIS TEST
1|5L6D	2|USE OF COCAINE DTMD BY OTHER THAN URINALYSIS TEST
1|5L6E	|GROWING OR MANUFACTURING OF COCAINE
1|5L5E	1|MFG W/INTENT TO DISTRIBUTR COCAINE
1|5L6F	|POSSESSION OF COCAINE WITH INTENT TO DISTRIBUTE
1|5L6G	|INTRODUCE OTHER COCAINE
1|5L6G	1|INTRODUCE W/INTENT TO DISTRIBUTE COCAINE
1|5L6H	|IMPORT AND/OR EXPORT OTHER COCAINE
|5M	|[PERJURY, FALSE SWEARING, FALSE OFFICIAL STMT]
|5M1	|PERJURY
|5M1A	|PERJURY: GIVING FALSE TESTIMONY
|5M1B	|PERJURY: SUBSCRIBING FALSE STATEMENT
|5M1C	PERJURY: SUBORNATION OF
|5M2	|FALSE SWEARING |
|5M3	|[FALSE OFFICIAL STATEMENT]
|5M3A	|FALSE OFFICIAL STMT NOT TO FINANCE, PERSONNEL, ETC
|5M3B	|FALSE OFFICIAL STATEMENT TO A FINANCE ACTIVITY
|5M3C	|FALSE OFFICIAL STATEMENT TO A PERSONNEL ACTIVITY
|5M3D	|FALSE OFFICIAL STATEMENT TO A COMMISSARY ACTIVITY
|5M3E	|[FALSE OFFICIAL STATEMENT TO PROCUREMENT ACTIVITY]
|5M3E1	|FALSE OFFICIAL STMT REGARDING PROGRESS PAYMENTS
|5M3E2	|FALSE OFFICIAL STMT REGARDING FAST PAY PROCEDURES
|5M3E3	|FALSE OFFICIAL STMT REGARDING RFP/IFB
|5M3E4	|FALSE OFFICIAL STMT REGARDING COST AND PRICE DATA
|5M3E5	|FALSE OFFICIAL STMT REGARD CONTRACT NEGOTIATIONS
|5M3E6	|FALSE OFFICIAL STMT REGARDING DEFECTIVE MATERIALS
|5M3E7	|FALSE OFFICIAL STMT/RELEASE OF PROPRIETARY INFO
|5M3F	|FALSE OFFICIAL STMT SUBMITTED TO AN AAFES ACTIVITY
|5M3G	|FALSE OFFICIAL STMT SUBMITTED-NAF INSTRUMENTALITY
|5M3H	|FALSE OFFICIAL STMT TO PROPERTY DISPOSAL ACTIVITY

|5M3H |FALSE OFFICIAL STMT TO PROPERTY DISPOSAL ACTIVITY
|5M3J |FALSE OFFICIAL STMT - WORKMEN COMPENSATION CLAIMS
|5M3K |FALSE OFFICIAL STATEMENT REGARDING CHAMPUS CLAIMS
|5P1 |SIGN FALSE DOCUMENT
|5P2 |FALSE OFFICAL STATEMENT|
|5M4 |[FALSE CLAIMS (CHARGEABLE UNDER 18 USC)]
|5M4A |FALSE CLAIM NOT TO FINANCE, PERSONNEL, AAFES, ETC
|5M4B |FALSE CLAIM SUBMITTED TO A FINANCE ACTIVITY
|5M4C |FALSE CLAIM SUBMITTED TO A PERSONNEL ACTIVITY
|5M4D |FALSE CLAIM SUBMITTED TO A COMMISSARY ACTIVITY
|5M4E |[FALSE CLAIM SUBMITTED TO A PROCUREMENT ACTIVITY]
|5M4E1 |FALSE CLAIM REGARDING PROGRESS PAYMENTS
|5M4E2 |FALSE CLAIM REGARDING FAST PAY PROCEDURES
|5M4E3 |FALSE CLAIM REGARDING COST AND PRICE DATA
|5M4F |FALSE CLAIM SUBMITTED TO AN AAFES ACTIVITY
|5M4G |FALSE CLAIM SUBMITTED TO AN NAF INSTRUMENTALITY
|5M4H |FALSE CLAIM TO A PROPERTY DISPOSAL ACTIVITY
|5N |[ROBBERY]
|5N1 |ASSAULT W INTENT TO COMMIT ROBBERY/ATTMPTD ROBBERY
|5N2 |[ROBBERY OF AN INDIVIDUAL]
|5N2A |[ROBBERY OF AN INDIVIDUAL WITH A HANDGUN]
|5N2A1 |ROBBERY OF INDIVIDUAL W/HANDGUN BY AN INDIVIDUAL
|5N2A2 |ROBBERY OF INDIVIDUAL W/HANDGUN BY 1+ INDIVIDUALS
|5N2A2 |ROBBERY OF INDIVIDUAL W/HANDGUN BY 1+ INDIVIDUALS
|5N2B |[ROBBERY OF AN INDIVIDUAL WITH A SHOULDER WEAPON]
|5N2B1 |ROBBERY OF INDIVIDUAL W/SHOULDER WEAPON BY INDIVID
|5N2B2 |ROBBERY OF INDIVIDUAL W/SHOULDER WEAPON BY 1+ IND
|5N2C |[ROBBERY OF AN INDIVIDUAL WITH A KNIFE/KNIVES]
|5N2C1 |ROBBERY OF INDIVIDUAL WITH KNIFE BY AN INDIVIDUAL
|5N2C2 |ROBBERY OF INDIVIDUAL W/KNIFE BY MORE THAN ONE IND
|5N2D |[ROBBERY OF INDIVIDUAL USING STRONG-ARM METHODS]
|5N2D1 |ROBBERY OF INDIVIDUAL USING STRONG-ARM BY INDIVID
|5N2D2 |ROBBERY OF INDIVIDUAL USING STRONG-ARM BY 1+ IND
|5N2E |[ROBBERY OF AN INDIVIDUAL USING OTHER METHODS]
|5N2E1 |ROBBERY OF INDIVIDUAL USING OTR METHODS BY INDIVID
|5N2E2 |ROBBERY OF INDIVIDUAL USING OTR METHODS BY 1+ IND
|5N3 |[ROBBERY OF A BUSINESS (BANK, STORE, ETC)]
|5N3A |[ROBBERY OF A BUSINESS WITH A HANDGUN]
|5N3A1 |ROBBERY OF A BUSINESS WITH A HANDGUN BY INDIVIDUAL
|5N3A2 |ROBBERY OF BUSINESS W/HANDGUN BY MORE THAN ONE IND

|5N3B |[ROBBERY OF A BUSINESS WITH A SHOULDER WEAPON]
|5N3B1 |ROBBERY OF BUSINESS W/SHOULDER WEAPON BY INDIVID
|5N3B2 |ROBBERY OF BUSINESS W/SHOULDER WEAPON BY 1+ IND
|5N3C |[ROBBERY OF A BUSINESS WITH A KNIFE/KNIVES]
|5N3C |[ROBBERY OF A BUSINESS WITH A KNIFE/KNIVES]
|5N3C1 |ROBBERY OF BUSINESS WITH A KNIFE BY AN INDIVIDUAL
|5N3C2 |ROBBERY OF BUSINESS W/KNIFE BY MORE THAN ONE IND
|5N3D |[ROBBERY OF A BUSINESS USING STRONG-ARM METHODS]
|5N3D1 |ROBBERY OF BUSINESS USING STRONG-ARM BY INDIVIDUAL
|5N3D2 |ROBBERY OF BUSINESS USING STRONG-ARM BY 1+ INDIVID
|5N3E |[ROBBERY OF A BUSINESS USING OTHER MEANS]
|5N3E1 |ROBBERY OF BUSINESS USING OTR MEANS BY AN INDIVID
|5N3E2 |ROBBERY OF BUSINESS USING OTR MEANS BY 1+ INDIVID
|5N4 |ROBBERY: WITH FIREARM
|5N5 |ROBBERY: OTHER CASE
|5P |[SUICIDE]
|5P1 |SUICIDE (ATTEMPTED)
|5P2 |[SUICIDE (SUCCESSFUL)]
|5P2A |[SUICIDE OF A MINOR DEPENDENT (UNDER 18)]
|5P2A1 |SUICIDE OF A MINOR DEPENDENT BY SHOOTING
|5P2A2 |SUICIDE OF A MINOR DEPENDENT BY HANGING
|5P2A3 |SUICIDE OF A MINOR DEPENDENT BY DROWNING
|5P2A4 |SUICIDE OF MINOR DEPENDENT BY POISONING(DRUGS ETC)
|5P2A5 |SUICIDE OF MINOR DEPENDENT BY CUTTING, STABBING
|5P2A6 |SUICIDE OF A MINOR DEPENDENT BY OTHER MEANS
|5P2B |[SUICIDE OF AN ADULT DEPENDENT (18 AND OVER)]
|5P2B1 |SUICIDE OF AN ADULT DEPENDENT BY SHOOTING
|5P2B1 |SUICIDE OF AN ADULT DEPENDENT BY SHOOTING
|5P2B2 |SUICIDE OF AN ADULT DEPENDENT BY HANGING
|5P2B3 |SUICIDE OF AN ADULT DEPENDENT BY DROWNING
|5P2B4 |SUICIDE OF ADULT DEPENDENT BY POISONING(DRUGS ETC)
|5P2B5 |SUICIDE OF ADULT DEPENDENT BY CUTTING, STABBING
|5P2B6 |SUICIDE OF AN ADULT DEPENDENT BY OTHER MEANS
|5P2C |[SUICIDE OF AN ENLISTED SOLDIER]
|5P2C1 |SUICIDE OF AN ENLISTED SOLDIER BY SHOOTING
|5P2C2 |SUICIDE OF AN ENLISTED SOLDIER BY HANGING
|5P2C3 |SUICIDE OF AN ENLISTED SOLDIER BY DROWNING
|5P2C4 |SUICIDE OF ENLISTED SOLDIER BY POISONING(DRUGS ETC
|5P2C5 |SUICIDE OF ENLISTED SOLDIER BY CUTTING, STABBING
|5P2C6 |SUICIDE OF AN ENLISTED SOLDIER BY OTHER MEANS
|5P2D |[SUICIDE OF AN OFFICER]
|5P2D1 |SUICIDE OF AN OFFICER BY SHOOTING
|5P2D2 |SUICIDE OF AN OFFICER BY HANGING

|5P2D3 |SUICIDE OF AN OFFICER BY DROWNING
|5P2D4 |SUICIDE OF AN OFFICER BY POISONING (DRUGS, ETC)
|5P2D5 |SUICIDE OF AN OFFICER BY CUTTING, STABBING, ETC
|5P2D6 |SUICIDE OF AN OFFICER BY OTHER MEANS
|5P2E |[SUICIDE OF OTHER PERSONNEL]
|5P2E |[SUICIDE OF OTHER PERSONNEL]
|5P2E1 |SUICIDE OF OTHER PERSONNEL BY SHOOTING
|5P2E2 |SUICIDE OF OTHER PERSONNEL BY HANGING
|5P2E3 |SUICIDE OF OTHER PERSONNEL BY DROWNING
|5P2E4 |SUICIDE OF OTHER PERSONNEL BY POISONING(DRUGS ETC)
|5P2E5 |SUICIDE OF OTHER PERSONNEL BY CUTTING, STABBING ..
|5P2E6 |SUICIDE OF OTHER PERSONNEL BY OTHER MEANS
|5P3 |SUICIDE (GESTURE)
|5Q |[TRAFFIC]
|5Q1 |TRAFFIC FATALITY
|5Q2 |DRUNKEN DRIVING
|5Q2A |DRUNK DRIVING: PERSONAL INJURY
|5Q2B |DRUNK DRIVING: OTHER CASES
|5Q3 |FLEEING THE SCENE OF A TRAFFIC ACCIDENT
|5Q4 |[TRAFFIC ACCIDENT-INJURY/DESTRUCTION OF PROPERTY]
|5Q4A |TRAFFIC ACCIDENT RESULTING IN PERSONAL INJURY
|5Q4B |[TRAFFIC ACCIDENT RESULTING IN DAMAGE TO PROPERTY]
|5Q4B1 |TRAFFIC ACCIDENT WITH DAMAGE TO GOVT PROPERTY
|5Q4B2 |TRAFFIC ACCIDENT WITH DAMAGE TO PRIVATE PROPERTY
|5Q5 |TRAFFIC VIOLATIONS, OTHER
|5Q5A |CARELESS OR RECKLESS DRIVING
|5Q5A1 |RECKLESS DRIVING: PERSONAL INJURY
|5Q5A2 |RECKLESS DRIVING:OTHER CASES
|5Q6 |TRAFFIC ACCIDENT W/O INJURY/DAMAGE TO PROPERTY
|5Q9 |ALCOHOL/DRUG RELATED TRAFFIC OFFENSES
|5Q9 |ALCOHOL/DRUG RELATED TRAFFIC OFFENSES
|5R |[WEAPONS VIOLATIONS]
|5R1 |[CONCEALED WEAPONS]
|5R1A |CARRYING A CONCEALED PISTOL/REVOLVER
|5R1B |CARRYING CONCEALED KNIFE, RAZOR,CUTTING INSTRUMENT
|5R1C |CARRYING A CONCEALED BLACKJACK
|5R1D |CARRYING A CONCEALED SHOTGUN
|5R1E |CARRYING A CONCEALED RIFLE
|5R1F |CARRYING A CONCEALED SUBMACHINE GUN
|5R2 |[UNLAWFUL POSSESSION OF WEAPONS]
|5R2A |UNLAWFUL POSSESSION OF A PISTOL/REVOLVER
|5R2B |UNLAWFUL POSSESSION OF KNIFE, RAZOR, CUTTING INSTR

|5R2C |UNLAWFUL POSSESSION OF A BLACKJACK
|5R2D |UNLAWFUL POSSESSION OF A SHOTGUN
|5R2E |UNLAWFUL POSSESSION OF A RIFLE
|5R2F |UNLAWFUL POSSESSION OF A SUBMACHINE GUN
|5R2G |WRONGFUL POSSESSION OF EXPLOSIVES & DEVICES
|5R3 |OTHER WEAPON MATTERS
|5R4A |FIREARM: DISCHARGE, NEGLECT
|5R4B |FIREARM: DISCHARGE, WILFUL
|5R4C |WEAPON: CARRYING CONCEALED
|5S |[ESCAPE]
|5S1 |ESCAPE FROM CONFINEMENT
|5S1A |ESCAPE FROM PRETRIAL CONFINEMENT
|5S1B |ESCAPE FROM POSTTRIAL CONFINEMENT
|5S1C |RELEASE PRISONER WITHOUT AUTHORITY
|5S1D |ALLOW ESCAPE: NEGLECT
|5S1E |ALLOW ESCAPE: DESIGN
|5S1F |PRISONER: ALLOWING TO DO UNAUTHORIZED ACT
|5S2 |ESCAPE FROM CUSTODY
|5S2A |ESCAPE FROM CUSTODY
|5S2B |ESCAPE FROM CORRECTIONAL CUSTODY
|5S2C | BREACH OF CORRECTIONAL CUSTODY
|5S3 |RESISTING/BREAKING
|5S3A |RESISTING APPREHENSION
|5S3B |RESISTING ARREST (CIVIL)
5S3C |BREAK ARREST
5S3D |RESTRICTION BREAKING
5S3E |BREAK QUARATINE
5S4 |UNLAWFUL DETENTION
5S5 |PAROLE: VIOLIATION
|5T |[COMMUNICATIONS INCIDENTS]
|5T1 |COMMUNICATING A THREAT (OTHER THAN TELEPHONE)
|5T2 |TELEPHONE THREATS
|5T3 |BOMB THREATS (ALL TYPES)
|5T4 |THREAT: COMMUNICATE
|5U |[HARASSING COMMUNICATION]
|5U1 |HARASSING COMMUNICATION
|5U2 |HARASSING COMMUNICATION BY TELEPHONE
|5V |MALINGERING
|5V1 |MALINGER: TIME OF WAR
|5V2 |MALINGER: OTHER
|5V3 |INJURE SELF: TIME OF WAR
|5V3 |INJURE SELF: OTHER
|5W |[UNAUTHORIZED ABSENCES]
|5W1 |DESERTION
|5W1A |DESERTION, SURRENDERED
|5W1B |DESERTION, APPREHENDED BY MILITARY

|5W1C |DESERTION, APPREHENDED BY CIVILIAN
|5W1D |DESERT: AVOID DUTY
|5W1E |DESERT: TERMINATE BY APPREHENSION
|5W1F |DESERT: OTHERWISE TERMINATE
|5W1G |DESERT: BEFORE NOTICE: APPREHEND
|5W1H |DESERT: BEFORE NOTICE: OTHER
|5W1J |DESERT: IN TIME OF WAR
|5W1K |SOLICIT: DESERT
|5W2 |AWOL
|5W2A |AWOL, SURRENDERED
|5W2B |AWOL, APPREHENDED BY MILITARY
|5W2C |AWOL, APPREHENDED BY CIVILIAN
|5W2D |AWOL: FROM PLACE OF DUTY
|5W2E |AWOL: TO PLACE OF DUTY
|5W2F |AWOL: 3 DAYS OR LESS
|5W2G |AWOL: OVER 3 LESS THAN 30 DAYS
|5W2H |AWOL: OVER 30 DAYS
|5W2J |AWOL: OVER 30 APPREHENDED
|5W2K |AWOL: WATCH OR GUARD
|5W2L |AWOL: INTENT TO ABANDON
|5W2M |AWOL: AVOID MANEUVERS
|5W2N |MISS MOVEMENT:DESIGN
|5W2O |MISS MOVEMENT: NEGLECT
|5W2P |JUMP VESSEL
|5X |[OTHER OFFENSES AGAINST PERSONS]
|5X |[OTHER OFFENSES AGAINST PERSONS]
|X1 |CONSPIRACY
|5X2 |SOLICITATION TO COMMIT AN OFFENSE
|5X3 |ACCESSORY BEFORE THE FACT
|5X4 |ACCESSORY AFTER THE FACT
|5X5 |OBSTRUCTION OF JUSTICE
|5X6 |MISPRISON: SERIOUS OFFENSE
|5X7 |REQUEST COMMISSION OF OFFENSE
|5Y |[CONDUCT UNBECOMING A MEMBER OF THE MILITARY SVC]
|5Y1 |DRUNK & DISORDERLY
|5Y1A |DRUNK IN PUBLIC
|5Y1A1 |DRINKING UNDERAGE WITH PERMISSION
|5Y1A2 |DRINKING UNDERAGE WITHOUT PERMISSION
|5Y1B |DRUNK ON DUTY
|5Y1B1 |DRINKING UNDERAGE WITH PERMISSION
|5Y1B2 |DRINKING UNDERAGE WITHOUT PERMISSION
|5Y1B3 |DRUNK: UNABLE TO PERFORM DUTIES
|5Y1B4 |DRUNK: ABOARD SHIP
|5Y1B5 |DRUNK: OTHER CASE
|5Y1B6 |DRUNK/DISORDERLY: OTHER CASES

|5Y1B7 |DRUNK/DISORDERLY: BRING DISCREDIT
|5Y1B8 |DRUNK/DISORDERLY: OTHER
|5Y1C |[PRISONER DRINKING]
|5Y1C1 |DRINK LIQUOR WITH PRISONER
|5Y1C2 |DRUNK PRISONER
|5Y1D |[DISORDERLY CONDUCT]
|5Y1D1 |DISORDERLY CONDUCT: BRING DISCREDIT
|5Y1D2 |DISORDERLY CONDUCT: OTHER CASES
|5Y2 |MISCONDUCT (OTHER THAN DRUNK & DISORDERLY)
|5Y2A |[CONTEMPT/DISRESPECT/DISOBEY]
|5Y2A1 |CONTEMPT TOWARDS OFFICIAL
|5Y2A2 |DISRESPECT TOWARDS SUPERIOR
|5Y2A3 |DISRESPECT: WARRANT OFFICER
|5Y2A4 |DISRESPECT: SUPERIOR NCO/PO
|5Y2A5 |DISRESPECT: OTHER NCO/PO
|5Y2A6 |DISOBEY: LAWFUL ORDER OF COMM OFFICER
|5Y2A7 |DISOBEY: IN TIME OF WAR
|5Y2A8 |DISOBEY: WARRANT OFFICER
|5Y2A9 |DISOBEY: NCO OR PO
5Y2B |[FAIL TO OBEY GENERAL ORDER]
|5Y2B0 |FAIL TO OBEY GENERAL ORDER: OTHER
|5Y2B1 |FAIL TO OBEY GENERAL ORDER: APPEARANCE
|5Y2B2 |FAIL TO OBEY GENERAL ORDER: BLACK MARKET
|5Y2B3 |FAIL TO OBEY GENERAL ORDER: FRATERNIZATION
|5Y2B4 |FAIL TO OBEY GENERAL ORDER: PARAPHERNALIA
|5Y2B5 |FAIL TO OBEY GENERAL ORDER: SECURITY
|5Y2B6 |FAIL TO OBEY GENERAL ORDER: SEXUAL HARASSMENT
|5Y2B7 |FAIL TO OBEY GENERAL ORDER: STANDARDS OF CONDUCT
|5Y2B8 |FAIL TO OBEY GENERAL ORDER: TRAFFIC
|5Y2B9 |FAIL TO OBEY GENERAL ORDER: WEAPONS
|5Y2C |FAIL TO OBEY OTHER ORDER
|5Y2D |[DERELICT DUTIES]
|5Y2D1 |DERELICT DUTIES: NEGLECT
|5Y2D2 |DERELICT DUTIES: WILLFUL
|5Y2E |CRUELTY OF SUBORDINATES
|5Y2F |DUELING
|5Y2G |[CONDUCT UNBECOMING OFFICER]
|5Y2G1 |CONDUCT UNBECOMING OFFICER: COPY/CHEAT
|5Y2G2 |CONDUCT UNBECOMING OFFICER: DRUNK/DISORDERLY
|5Y2G3 |CONDUCT UNBECOMING OFFICER: FRATERNIZATION
|5Y2G4 |CONDUCT UNBECOMING OFFICER: OTHER
|5Y2H |ABUSING ANIMIAL
|5Y2J |[PROCEDURAL RULES]
|5Y2J1 |DELAY DISPOSITION OF CASE
|5Y2J2 |FAIL TO ENFORCE PROCEDURAL RULE

|5Y2J3 |WRONGFUL INTERFERENCES W/ADMIN PROCEEDINGS
|5Y2J4 |PUBLIC RECORD: ALTER/REMOVE
|5Y2J5 |REFUSE TO TESTIFY
|5Y2K |[SENTINEL MISCONDUCT]
|5Y2K1 |MISBEHAVE: SENTINEL IN WAR
|5Y2K2 |MISBEHAVE: SENTINEL WITH SPECIAL PAY
|5Y2K3 |MISBEHAVE: SENTINEL OTHER PLACES
|5Y2K4 SENTINEL: DISRESPECT
|5Y2K5 SENTINEL: LOITERING IN TIME OF WAR
|5Y2K6 SENTIMEL : LOITERING AT OTHER TIMES
|5Y2L | MUTINY
|5Y2L1 |SOLICIT: MUTINY
|5Y2L2 |MUTINY: BY VIOLENCE OR DISTURBANCE
|5Y2L3 |MUTINY: REFUSING TO OBEY ORDERS OR PERFORM DUTY
|5Y2L4 |MUTINY: FAILURE TO PREVENT OR SUPPRESS
|5Y2L5 |MUTINY: FAILURE TO REPORT
|5Y2M |[SEDITION]
|5Y2M1 |SOLICIT: SEDITION
|5Y2M2 |SEDITION:
|5Y2M3 |SEDITION: FAILUTURE TO PREVENT OR SUPPRESS
|5Y2M4 |SEDITION: FAILURE TO REPORT
|5Y2N |[MISCONDUCT BEFORE ENEMY]
|5Y2N1 1|BEFORE ENEMY: RUN AWAY
|5Y2N2 2|BEFORE ENEMY: SHAMEFUL ABANDON/SURRENDER/DELIVER
|5Y2N3 3|BEFORE ENEMY: ENDANGER COMMAND/UNIT/PLACE/SHIP
|5Y2N4 4|BEFORE ENEMY: CAST AWAY ARMS OR AMMUNITION
|5Y2N5 5|BEFORE ENEMY: COWARDLY CONDUCT
|5Y2N6 6|BEFORE ENEMY: QUIT PLACE OF DUTY TO PLUNDER/PILLA
|5Y2N7 7|BEFORE ENEMY:CAUSE FALSE ALARM
|5Y2N8 8|BEFORE ENEMY: WILLFUL FAILURE TO ENCOUNTER ENEMY
|5Y2N9 9|BEFORE ENEMY: FAIL TO AFFORD RELIEF OR ASSISTANCE
|5Y2O |[OTHER OFFENSE BEFORE ENEMY]
|5Y2O1 |COMPEL SURRENDER
|5Y2O2 |STRIKE FLAG BEFORE ENEMY
|5Y2O3 |DISCLOSE PAROLE/COUNTERSIGN TO UNAUTHORIZED
|5Y2O4 |GIVE PAROLE/COUNTERSIGN DIFFERENT FROM AUTHORIZED
|5Y2O5 |FORCING SAFEGUARD
|5Y2O6 |STRAGGLING
|5Y2P |[SPYING/ESPIONAGE/AIDING ENEMY]
|5Y2P1 |SPYING
|5Y2P2 |ESPIONAGE
|5Y2P3 |DISLOYAL STATEMENT
|5Y2P4 |AIDING THE ENEMY

|5Y2P5 |HARBORING OR PROTECTING ENEMY
|5Y2P6 |GIVING INTELLIGENCE TO ENEMY
|5Y2P7 |COMMUNICATING WITH ENEMY
|5Y2P8 |MISCONDUCT AS POW: FOR FAVORABLE TREATMENT
|5Y2P9 |MISCONDUCT AS POW: MALTREAT PRISONER
|5Y2Q |LOOTING, PILLAGING
|5Y3 |RIOT
|5Y3A |BREACH OF PEACE
|5Y3B |PROVOKING SPEECH/GESTURES
|5Z |[CRIMINAL TERRORISM/TERRORISM ACTS]
|5Z1 |[CRIMINAL TERRORISM TARGETED AGAINST PERSON]
|5Z1A |[TERRORIST THREATS AGAINST PERSONS]
|5Z1A1 |TERRORIST THREATS AGAINST PERSONS BY MAIL
|5Z1A2 |TERRORIST THREATS AGAINST PERSONS BY TELEPHONE
|5Z1A2 |TERRORIST THREATS AGAINST PERSONS BY TELEPHONE
|5Z1A3 |TERRORIST THREATS AGAINST PERSONS IN PERSON
|5Z1A4 |TER THREATS A/PERSONS BY COMB OF THREATS IN PERSON
|5Z1A5 |TER THREATS AGAINST PERSONS THROUGH INTERMEDIARY
|5Z1B |[CRIM TERRORISM A/PERSONS INVL EXPLOSIVE DEVICE]
|5Z1B1 |CRIM TERRORISM AGAINST PERSONS INVL TNT/DYNAMITE
|5Z1B2 |CRIM TERRORISM A/PERSONS INVOLVING GASOLINE ETC
|5Z1B3 |CRIM TERRORISM A/PERSONS INVL OTR EXPLOSIVE DEVICE
| 5Z1B4 |CRIM TERRORISM-DEVICE DISCOVERED BEFORE DETONATION
|5Z1B5 |CRIM TERRORISM-DEVICE DISCOVERED AFTER DETONATION
|5Z2 |[TERRORIST THREATS TARGETED AGAINST EQUIPMENT]
|5Z2A |[TERRORIST THREATS AGAINST EQUIPMENT]
|5Z2A1 |TERRORIST THREATS AGAINST EQUIPMENT BY MAIL
|5Z2A2 |TERRORIST THREATS AGAINST EQUIPMENT BY TELEPHONE
|5Z2A3 |TERRORIST THREATS AGAINST EQUIPMENT IN PERSON
|5Z2A4 |TER THREATS A/EQUIP (COMB THREATS IN PERSON)
|5Z2A5 |TER THREATS AGAINST EQUIPMENT THROUGH INTERMEDIARY
|5Z2B |[CRIM TERRORISM A/EQUIPMENT INVL EXPLOSIVE DEVICE
|5Z2B1 |CRIM TERRORISM AGAINST EQUIPMENT INVL TNT/DYNAMITE
|5Z2B2 |CRIM TERRORISM A/EQUIPMENT INVL GASOLINE ETC
|5Z2B3 |CRIM TERRORISM A/EQUIP INVL OTHER EXPLOSIVE DEVICE
|5Z2B3 |CRIM TERRORISM A/EQUIP INVL OTHER EXPLOSIVE DEVICE

|5Z2B4 |CRIM TERRORISM-DEVICE DISCOVERED BEFORE DETONATION
|5Z2B5 |CRIM TERRORISM-DEVICE DISCOVERED AFTER DETONATION
|5Z3 |[CRIMINAL TERRORISM TARGETED AGAINST FACILITIES]
|5Z3A |[TERRORIST THREATS AGAINST FACILITIES]
|5Z3A1 |TERRORIST THREATS AGAINST FACILITIES BY MAIL
|5Z3A2 |TERRORIST THREATS AGAINST FACILITIES BY TELEPHONE
|5Z3A3 |TERRORIST THREATS AGAINST FACILITIES IN PERSON
|5Z3A4 |TER THREATS A/FACILITIES COMB OF THREATS IN PERSON
|5Z3A5 |TER THREATS AGAINST FACILITIES THRU INTERMEDIARY
|5Z3B |[CRIM TERRORISM A/FACILITIES INV EXPLOSIVE DEVICE]
|5Z3B1 |CRIM TERRORISM A/FACILITIES INVOLVING TNT/DYNAMITE
|5Z3B2 |CRIM TERRORISM A/FACILITIES INVL GASOLINE ETC
|5Z3B3 |CRIM TERRORISM A/FAC INVL OTHER EXPLOSIVE DEVICE
|5Z3B4 |CRIM TERRORISM-DEVICE DISCOVERED BEFORE DETONATION
|5Z3B5 |CRIM TERRORISM-DEVICE DISCOVERED AFTER DETONATION
|5Z4 |[CRIM TERRORISM AGAINST MULTIPLE TARGETS, PER/EQU]
|5Z4A |[TERRORIST THREATS AGAINST MULTIPLE TARGETS]
|5Z4A1 |TERRORIST THREATS AGAINST MULTIPLE TARGETS BY MAIL
|5Z4A2 |TERRORIST THREATS AGAINST MULTIPLE TARGETS BY TELE
|5Z4A3 |TER THREATS AGAINST MULTIPLE TARGETS IN PERSON
|5Z4A3 |TER THREATS AGAINST MULTIPLE TARGETS IN PERSON
|5Z4A4 |TER THREATS A/MULTIPLE TARGETS(COMB OF THREATS)PER
|5Z4A5 |TER THREATS A/MULTIPLE TARGETS THRU INTERMEDIARY
|5Z4B |[CRIM TERRORISM A/MULTIPLE TARGETS INVL EXPLOSIVE]
|5Z4B1 |CRIM TERRORISM A/MULTIPLE TARGETS - TNT/DYNAMITE
|5Z4B2 |CRIM TERRORISM A/MULTIPLE TARGETS INV GASOLINE ETC
|5Z4B3 |CRIM TERRORISM A/TARGETS INVL OTR EXPLOSIVE DEVICE
|5Z4B4 |CRIM TERRORISM-DEVICE DISCOVERED BEFORE DETONATION
|5Z4B5 |CRIM TERRORISM-DEVICE DISCOVERED AFTER DETONATION

|6 |[SEX CRIMES]
|6A |[CHILD MOLESTATION]
|6A1 |INDECENT ASSAULT ON A CHILD (U125) (U134)
|6A2 |INDECENT ACTS UPON A CHILD (U134)
|6A3 |ENTICING A CHILD TO COMMIT A LEWD ACT (U134)

|6A4 |EXHIBITIONISM OR LEWD GESTURES TOWARD MINOR (134)
|6C |[INDECENT ACTS (NOT INVOLVING SODOMY)]
|6C1 |INDECENT ASSAULT
|6C2 |INDECENT ACTS BETWEEN TWO OR MORE MALES (U134)
|6C3 |INDECENT ACTS BETWEEN TWO OR MORE FEMALES (U134)
|6C4 |INDECENT ACTS BETWEEN MALES & FEMALES (U134)
|6C5 |INDECENT ACTS BETWEEN ADULTS & MINORS (U134)
|6C5 |INDECENT ACTS BETWEEN ADULTS & MINORS (U134)
|6D |[PORNOGRAPHY]
|6D1 |[PRODUCTION/PUBLICATION OF PORNOGRAPHY]
|6D1A |PRODUCTION OR PUBLICATION OF PORNOGRAPHIC ART
|6D1B |PRODUCTION OR PUBLICATION OF PORNO LITERATURE
|6D1C |PRODUCTION OR PUBLICATION OF PORNOGRAPHIC MOVIES
|6D1D |PRODUCTION OR PUBLICATION OF PORNO PHOTOGRAPHS
|6D2 |[SMUGGLING/ILLEGAL TRANSPORT OF PORNOGRAPHY]
|6D2A |SMUGGLING/ILLEGAL TRANSPORT OF PORNOGRAPHIC ART
|6D2B |SMUGGLING/ILLEGAL TRANSPORT OF PORNO LITERATURE
|6D2C |SMUGGLING/ILLEGAL TRANSPORT OF PORNOGRAPHIC MOVIES
|6D2D |SMUGGLING/ILLEGAL TRANSPORT OF PORNO PHOTOGRAPHS
|6D3 |[TRANSPORT OF PORNOGRAPHY (OTHER THAN SMUGGLING)]
|6D3A |ILLEGAL TRANSPORT OF PORNOGRAPHIC ART
|6D3B |ILLEGAL TRANSPORT OF PORNOGRAPHIC LITERATURE
|6D3C |ILLEGAL TRANSPORT OF PORNOGRAPHIC MOVIES
|6D3D |ILLEGAL TRANSPORT OF PORNOGRAPHIC PHOTOGRAPHS
|6D4 |[INTRODUCTION OF PORNOGRAPHY INTO MAIL CHANNELS]
|6D4A |INTRODUCTION OF PORNO ART INTO MAIL CHANNELS
|6D4B |INTRO OF PORNO LITERATURE INTO MAIL CHANNELS
|6D4C |INTRODUCTION OF PORNO MOVIES INTO MAIL CHANNELS
|6D4C |INTRODUCTION OF PORNO MOVIES INTO MAIL CHANNELS
|6D4D |INTRO OF PORNO PHOTOGRAPHS INTO MAIL CHANNELS
|6D5 |[ILLEGAL SALE OF PORNOGRAPHY]
|6D5A |ILLEGAL SALE OF PORNOGRAPHIC ART
|6D5B |ILLEGAL SALE OF PORNOGRAPHIC LITERATURE
|6D5C |ILLEGAL SALE OF PORNOGRAPHIC MOVIES
|6D5D |ILLEGAL SALE OF PORNOGRAPHIC PHOTOGRAPHS
|6D6 |[ILLEGAL EXHIBITION OF PORNOGRAPHY]
|6D6A |ILLEGAL EXHIBITION OF PORNOGRAPHIC ART
|6D6B |ILLEGAL EXHIBITION OF PORNOGRAPHIC LITERATURE
|6D6C |ILLEGAL EXHIBITION OF PORNOGRAPHIC MOVIES
|6D6D |ILLEGAL EXHIBITION OF PORNOGRAPHIC PHOTOGRAPHS
|6D7 |[ILLEGAL POSSESSION OF PORNOGRAPHY]
|6D7A |ILLEGAL POSSESSION OF PORNOGRAPHIC ART

|6D7B |ILLEGAL POSSESSION OF PORNOGRAPHIC LITERATURE
|6D7C |ILLEGAL POSSESSION OF PORNOGRAPHIC MOVIES
|6D7D |ILLEGAL POSSESSION OF PORNOGRAPHIC PHOTOGRAPHS
|6E |[RAPE & CARNAL KNOWLEDGE]
|6E1 |[RAPE]
4|6E1A |ASSAULT: WITH INTENT TO RAPE [ATTEMPTED RAPE]
|6E1A1 |ATTEMPTED RAPE BY FORCE (U120)
|6E1A1 |ATTEMPTED RAPE BY FORCE (U120)
|6E1A2 |ATTEMPTED RAPE BY FORCE WITH A WEAPON (U120)
|6E1A3 |GROUP RAPE OF AN ADULT (U120)
|6E1B |[RAPE OF A CHILD]
|6E1B1 |RAPE OF A CHILD BY FORCE (U120)
|6E1B2 |RAPE OF A CHILD WITH A WEAPON (U120)
|6E1B3 |GROUP RAPE OF A CHILD (U120)
|6E1C |[RAPE OF A DEPENDENT WIFE]
|6E1C1 |RAPE OF A DEPENDENT WIFE BY FORCE (U120)
|6E1C2 |RAPE OF A DEPENDENT WIFE WITH A WEAPON (U120)
|6E1C3 |GROUP RAPE OF A DEPENDENT WIFE (U120)
|6E1D |[RAPE OF A FOREIGN NATIONAL]
|6E1D1 |RAPE OF A FOREIGN NATIONAL BY FORCE (U120)
|6E1D2 |RAPE OF A FOREIGN NATIONAL WITH A WEAPON (U120)
|6E1D3 |GROUP RAPE OF A FOREIGN NATIONAL (U120)
|6E1E |[RAPE OF AN ENLISTED WOMAN]
|6E1E1 |RAPE OF AN ENLISTED WOMAN BY FORCE (U120)
|6E1E2 |RAPE OF AN ENLISTED WOMAN WITH A WEAPON (U120)
|6E1E3 |GROUP RAPE OF AN ENLISTED WOMAN (U120)
|6E1F |[RAPE OF A FEMALE OFFICER]
|6E1F1 |RAPE OF A FEMALE OFFICER BY FORCE (U120)
|6E1F1 |RAPE OF A FEMALE OFFICER BY FORCE (U120)
|6E1F2 |RAPE OF A FEMALE OFFICER WITH A WEAPON (U120)
|6E1F3 |GROUP RAPE OF A FEMALE OFFICER (U120)
|6E1G |[RAPE OF A FEMALE (OTHER)]
|6E1G1 |RAPE BY FORCE (OTHER) (U120)
|6E1G2 |RAPE WITH A WEAPON (OTHER) (U120)
|6E1G3 |GROUP RAPE (OTHER) (U120)
|6E2 |CARNAL KNOWLEDGE (U120)
1|6E2A |CARNAL KNOWLEDGE: CHILD 12 TO 16 YRS OLD
2|6E2B |CARNAL KNOWLEDGE: CHILD UNDER 12 YRS OLD
|6F |[SODOMY]
6|6F1 |[ASSAULT W/INTENT TO COMMIT/ATTEMPT SODOMY (U134)
|6F1A |HETEROSEXUAL
|6F1B |HOMOSEXUAL
|6F2 |[SODOMY/ACTIVE PARTICIPANT, FELLATIO (U125)]
|6F2A |HETEROSEXUAL
|6F2B |HOMOSEXUAL
|6F3 |[SODOMY/PASSIVE PARTICIPANT, FELLATIO (U125)]

|6F3A |HETEROSEXUAL
|6F3B |HOMOSEXUAL
|6F4 |[SODOMY/ACTIVE PARTICIPANT, ANAL (U125)]
|6F4A |HETEROSEXUAL
|6F4B |HOMOSEXUAL
|6F4B |HOMOSEXUAL
|6F5 |[SODOMY/PASSIVE PARTICIPANT, ANAL (U125)]
|6F5A |HETEROSEXUAL
|6F5B |HOMOSEXUAL
|6F6 |[SODOMY/ACTIVE PARTICIPANT, CUNNILINGUS (U125)]
|6F6A |HETEROSEXUAL
|6F6B |HOMOSEXUAL
|6F7 |[SODOMY/PASSIVE PARTICIPANT, CUNNILINGUS (U125)]
|6F7A |HETEROSEXUAL
|6F7B |HOMOSEXUAL
|6F8A |SODOMY: FORCE
|6F8B1 |SODOMY: CHILD 12 TO 16 YRS OLD
|6F8B2 |SODOMY: CHILD UNDER 12 YRS OLD
|6F8C |SODOMY: OTHER
|6G |BESTIALITY (U134)
|6H |EXHIBITIONISM
|6H1 |INDECENT EXPOSURE (U134)
|6J |[INCEST]
|6J1 |INCEST BY NATURAL PARENT (U134)
|6J2 |INCEST BY NATURAL BROTHER (U134)
|6J3 |INCEST BY NATURAL SISTER (U134)
|6K |[OBSCENE COMMUNICATION]
|6K1 |[TRANSMITTING OBSCENE TELEPHONE CALLS]
|6K1A |OBSCENE TELEPHONE CALLS TO OFF-POST NUMBERS (U134)
|6K1B |OBSCENE TELEPHONE CALLS TO ON-POST QUARTERS (U134)
|6K1B |OBSCENE TELEPHONE CALLS TO ON-POST QUARTERS (U134)
|6K1C |OBSCENE TELEPHONE CALLS TO OTHER ON-POST TELE
|6K2 |OBSCENE VERBAL COMMUNICATIONS (U134)
|6K2A |INDECENT LANGUAGE TO CHILD UNDER 16
|6K2B |INDECENT LANGUAGE: ALL OTHER
|6N |[CRIMINAL ABORTION]
|6N1 |CRIMINAL ABORTION BY A MEMBER OF THE ARMED FORCES
|6N2 |CRIMINAL ABORTION UPON FEMALE MEMBER ARMED FORCES
|6N3 |CRIMINAL ABORTION UPON ARMED FORCES FAMILY MEMBER
|6X |[OTHER SEX OFFENSES (U134)]

|6X1 |CONSPIRACY
|6X2 |SOLICITATION TO COMMIT AN OFFENSE
|6X3 |ACCESSORY BEFORE THE FACT
|6X4 |ACCESSORY AFTER THE FACT
|6X5 |OBSTRUCTION OF JUSTICE

|7 |[CRIMES AGAINST PROPERTY]
|7A |[ARSON]
|7A1 |[AGGRAVATED ARSON]
|7A1A |AGGRAVATED ARSON OF A DWELLING
|7A1B |AGGRAVATED ARSON OF A BUILDING
|7A1C |AGGRAVATED ARSON NOT A DWELLING
|7A1D |AGGRAVATED ARSON TO COVER A CRIME
|7A1E |AGGRAVATED ARSON FOR INSURANCE
|7A1E |AGGRAVATED ARSON FOR INSURANCE
|7A1F |ARSON: AGGRAVATED
|7A2 |[SIMPLE ARSON]
|7A2A |SIMPLE ARSON OF A DWELLING
|7A2B |SIMPLE ARSON OF A BUILDING
|7A2C |SIMPLE ARSON NOT A DWELLING
|7A2D |SIMPLE ARSON TO COVER A CRIME
|7A2E |SIMPLE ARSON FOR INSURANCE
|7A2F1 |ARSON:PROPERTY $100 OR LESS
|7A2F2 |ARSON:PROPERTY MORE THAN $100
|7A2G |ASSAULT: WITH INTENT ARSON
|7B |[BLACK-MARKET (CUSTOMS VIOLATIONS)]
|7B1 |[BLACK-MARKET OF NAF MERCHANDISE]
|7B1A |[BLACK-MARKET OF AAFES (PX) MERCHANDISE]
|7B1A1 |UNLAWFUL TRANSFER OF AAFES MERCHANDISE
|7B1A2 |UNLAWFUL POSSESSION OF AAFES MERCHANDISE
|7B1B |[BLACK-MARKET OF OPEN MESS MERCHANDISE]
|7B1B1 |UNLAWFUL TRANSFER OF OPEN MESS MERCHANDISE
|7B1B2 |UNLAWFUL POSSESSION OF OPEN MESS MERCHANDISE
|7B1C |[BLACK MARKET OF NAF PROPERTY (NOT 7B1A - 7B1B)]
|7B1C1 |UNLAWFUL TRANSFER OF NAF PROPERTY
|7B1C2 |UNLAWFUL POSSESSION OF NAF PROPERTY
|7B1D |[BLACK-MARKET OF OTHER ITEMS (NOT GOVT OR NAF]
|7B1D1 |UNLAWFUL TRANSFER OF OTHER NON-GOVERNMENT PROPERTY
|7B1D2 |UNLAWFUL POSSESSION OF OTHER NON-GOVT PROPERTY
|7B1D2 |UNLAWFUL POSSESSION OF OTHER NON-GOVT PROPERTY
|7B2 |[BLACK-MARKET OF GOVERNMENT PROPERTY]
|7B2A |UNLAWFUL TRANSFER OF GOVERNMENT PROPERTY
|7B2B |UNLAWFUL POSSESSION OF GOVERNMENT PROPERTY
|7B2C |[ITEMS IMPORTED IN HOLD BAGGAGE/HOUSEHOLD GOODS]
|7B2C1 |UNLAWFUL TRANSFER OF ITEMS IMPORTED IN

	BAGGAGE/HHG
|7B2C2	|UNLAWFUL POSSESS OF ITEMS IMPORTED IN BAGGAGE/HHG
|7B3	|[BLACK-MARKET OF COMMISSARY ITEMS]
|7B3A	|UNLAWFUL TRANSFER OF COMMISSARY ITEMS
|7B3B	|UNLAWFUL POSSESSION OF COMMISSARY ITEMS
|7B4	|[BLACK-MARKET OF POL ITEMS]
|7B4A	|UNLAWFUL TRANSFER OF POL ITEMS
|7B4B	|UNLAWFUL POSSESSION OF POL ITEMS
|7B5	|[BLACK-MARKET OF CLASS VI ITEMS]
|7B5A	|UNLAWFUL TRANSFER OF CLASS VI ITEMS
|7B5B	|UNLAWFUL POSSESSION OF CLASS VI ITEMS
|7B6	|[MISUSE OF APO/FPO TO IMPORT FOR BLACK MARKET]
|7B6A	|UNLAWFUL TRANSFER OF ITEMS IMPORTED THRU APO/FPO
|7B6B	|UNLAWFUL POSSESSION OF ITEMS IMPORTED THRU APO/FPO
|7B7	|UNLAWFUL CURRENCY TRANSACTIONS
|7B8	|ORGANIZED BLACK-MARKET OPERATIONS
|7B8	|ORGANIZED BLACK-MARKET OPERATIONS
|7B9	|ORGANIZED CURRENCY MANIPULATION
|7C	|[ILLEGAL ENTRY]
|7C1	|BURGLARY
|7C1A	|BURGLARY OF A BARRACKS
|7C1B	|BURGLARY OF A FAMILY DWELLING
|7C1C	|BURGLARY OF A HOUSE TRAILER
|7CID	|ASSAULT:WITH INTENT TO BURGLARY
|7C2	|[HOUSEBREAKING]
|7C2A	|HOUSEBREAKING OF A BARRACKS
|7C2B	|HOUSEBREAKING OF A FAMILY DWELLING
|7C2C	|HOUSEBREAKING OF A HOUSE TRAILER
|7C2D	|HOUSEBREAKING OF A TENT
|7C2E	|HOUSEBREAKING OF A WAREHOUSE
|7C2F	|HOUSEBREAKING, FINANCE OFFICES/BANKING FACILITIES
|7C2G	|HOUSEBREAKING OF A MESS HALLS (APPROPRIATED FUND)
|7C2H	|HOUSEBREAKING OF A EXCHANGE FACILITIES
|7C2J	|HOUSEBREAKING OF A NAF ACTIVITIES (NOT EXCHANGE)
|7C2K	|HOUSEBREAKING OF A ARMS STORAGE FACILITIES
|7C2L	|HOUSEBREAKING OF A COMMISSARY/GROCERY STORE
|7C2M	|HOUSEBREAKING OF A OFFICE FACILITIES
|7C2N	|HOUSEBREAKING, CLOTHING SALES STORES/DEPART/STORES
|7C2N	|HOUSEBREAKING, CLOTHING SALES STORES/DEPART/STORES
|7C2P	|HOUSEBREAKING, GASOLINE SALES/AUTO STORE/POL

	POINT
|7C2Q	|HOUSEBREAKING OF A BEVERAGE STORE &/OR TAVERNS
|7C2R	|HOUSEBREAKING OF A HARDWARE STORES
|7C2S	|HOUSEBREAKING OF AN EDUCATIONAL FACILITIES
|7C2T	|HOUSEBREAKING OF A UNIT SUPPLY FACILITIES
|7C2U	|HOUSEBREAKING OF A COMPUTER FACILITIES
|7C2X	|HOUSEBREAKING OF AN OTHER
|7C2V	|ASSAULT: WITH INTENT TO HOUSEBREAK
|7C3	|UNLAWFUL/FORCED ENTRY (INCLUDING AUTOMOBILES)
|7D	|[COUNTERFEITING]
|7D1	|[MANUFACTURE/PRODUCTION COUNTERFEIT INSTRUMENTS]
|7D1A	|COUNTERFEITING BONDS (U.S. GOVERNMENT)
|7D1B	|COUNTERFEITING CURRENCY (U.S.)
|7D1C	|COUNTERFEITING DOCUMENTS
|7D1D	|COUNTERFEITING FOREIGN CURRENCY
|7D1E	|COUNTERFEITING MILITARY PAYMENT CERTIFICATES
|7D1F	|COUNTERFEITING PASSES (INSTALLATION & SECURITY)
|7D1F1	|MILT PASS:WRONGFUL MAKE/TAMPER/ALERT/COUNTERFEIT
|7D1F2	|MILT PASS:WRONGFUL SALE/GIFT/LOAN/DISPOSITION
|7D1F3	|MILT PASS:WRONGFUL USE/POSSESS
|7D1F4	|MILT PASS: ALL OTHER
|7D1G	|COUNTERFEITING RATION DOCUMENTS (EXCEPT POL ITEMS)
|7D1H	|COUNTERFEITING TRANS CONTROL MOVEMENT DOCUMENTS
|7D1J	|COUNTERFEITING POL ITEM RATION DOCUMENTS
|7D1K	|COUNTERFEITING PAY & ALLOWANCES DOCUMENTS
|7D1K	|COUNTERFEITING PAY & ALLOWANCES DOCUMENTS
|7D1L	|COUNTERFEITING COMMISSARY DOCUMENTS
|7D1M	|COUNTERFEITING PROCUREMENT DOCUMENTS
|7D1N	|COUNTERFEITING PROPERTY DISPOSAL DOCUMENTS
|7D1P	|COUNTERFEITING NAF DOCUMENTS (EXCEPT RATION CARDS)
|7D2	|[TRAFFICKING IN COUNTERFEIT INSTRUMENTS]
|7D2A	|TRAFFICKING IN COUNTERFEIT BONDS (U.S. GOVERNMENT)
|7D2B	|TRAFFICKING IN COUNTERFEIT CURRENCY (U.S.)
|7D2C	|TRAFFICKING IN COUNTERFEIT DOCUMENTS
|7D2D	|TRAFFICKING IN COUNTERFEIT FOREIGN CURRENCY
|7D2E	|TRAFF IN COUNTERFEIT MILITARY PAYMENT CERTIFICATES
|7D2F	|TRAFF IN COUNTERFEIT PASSES(INSTALLATION/SECURITY)
|7D2G	|TRAFF IN COUNTERFEIT RATION DOCUMENTS (EXCEPT POL)
|7D2H	|TRAFF IN COUNTERFEIT TRANS CONTROL MOVEMENT DOC

|7D2J |TRAFF IN COUNTERFEIT POL ITEMS RATION DOCUMENTS
|7D2K |TRAFF IN COUNTERFEIT PAY & ALLOWANCES DOCUMENTS
|7D2L |TRAFFICKING IN COUNTERFEIT COMMISSARY DOCUMENTS
|7D2M |TRAFFICKING IN COUNTERFEIT PROCUREMENT DOCUMENTS
|7D2N |TRAFF IN COUNTERFEIT PROPERTY DISPOSAL DOCUMENTS
|7D2P |TRAFF IN COUNTERFEIT NAF DOC (NOT RATION CARDS)
|7D3 |[PASSING COUNTERFEIT INSTRUMENTS]
|7D3 |[PASSING COUNTERFEIT INSTRUMENTS]
|7D3A |PASSING COUNTERFEIT BONDS (U.S. GOVERNMENT)
|7D3B |PASSING COUNTERFEIT CURRENCY (U.S.)
|7D3C |PASSING COUNTERFEIT DOCUMENTS
|7D3D |PASSING COUNTERFEIT FOREIGN CURRENCY
|7D3E |PASSING COUNTERFEIT MILITARY PAYMENT CERTIFICATES
|7D3F |PASSING COUNTERFEIT PASSES (INSTALLATION/SECURITY)
|7D3G |PASS COUNTERFEIT RATION DOCUMENTS (NOT POL ITEMS)
|7D3H |PASS COUNTERFEIT TRANS CONTROL MOVEMENT DOCUMENTS
|7D3J |PASSING COUNTERFEIT POL ITEM RATION DOCUMENTS
|7D3K |PASSING COUNTERFEIT PAY & ALLOWANCES DOCUMENTS
|7D3L |PASSING COUNTERFEIT COMMISSARY DOCUMENTS
|7D3M |PASSING COUNTERFEIT PROCUREMENT DOCUMENTS
|7D3N |PASSING COUNTERFEIT PROPERTY DISPOSAL DOCUMENTS
|7D3P |PASS COUNTERFEIT NAF DOCUMENTS (NOT RATION CARDS)
|7D4 |[POSSESSION OF COUNTERFEIT INSTRUMENTS]
|7D4A |POSSESSION OF COUNTERFEIT BONDS (U.S. GOVERNMENT)
|7D4B |POSSESSION OF COU
|7D4C |POSSESSION OF COUNTERFEIT DOCUMENTS
|7D4D |POSSESSION OF COUNTERFEIT FOREIGN CURRENCY
|7D4E |POSS OF COUNTERFEIT MILITARY PAYMENT CERTIFICATES
|7D4E |POSS OF COUNTERFEIT MILITARY PAYMENT CERTIFICATES
|7D4F |POSS OF COUNTERFEIT PASSES (INSTALLATION/SECURITY)
|7D4G |POSS OF COUNTERFEIT RATION DOC (NOT POL ITEMS)
|7D4H |POSS OF COUNTERFEIT TRANS CONTROL MOVEMENT DOC
|7D4J |POSS OF COUNTERFEIT POL ITEM RATION DOCUMENTS
|7D4K |POSS OF COUNTERFEIT PAY & ALLOWANCES DOCUMENTS
|7D4L |POSSESSION OF COUNTERFEIT COMMISSARY DOCUMENTS
|7D4M |POSSESSION OF COUNTERFEIT PROCUREMENT

	DOCUMENTS
|7D4N	|POSS OF COUNTERFEIT PROPERTY DISPOSAL DOCUMENTS
|7D4P	|POSS OF COUNTERFEIT NAF DOC (NOT RATION CARDS)
|7D5	|[USE COUNTERFEIT INSTRUMENTS W/INTENT TO DECEIVE]
|7D5A	|USE OF COUNTERFEIT BONDS (U.S. GOVERNMENT)
|7D5B	|USE OF COUNTERFEIT CURRENCY (U.S.)
|7D5C	|USE OF COUNTERFEIT DOCUMENTS
|7D5D	|USE OF COUNTERFEIT FOREIGN CURRENCY
|7D5E	|USE OF COUNTERFEIT MILITARY PAYMENT CERTIFICATES
|7D5F	|USE OF COUNTERFEIT PASSES (INSTALLATION/SECURITY)
|7D5G	|USE OF COUNTERFEIT RATION DOC (EXCEPT POL ITEMS)
|7D5H	|USE OF COUNTERFEIT TRANS CONTROL MOVEMENT DOC
|7D5J	|USE OF COUNTERFEIT POL ITEM RATION DOCUMENTS
|7D5K	|USE OF COUNTERFEIT PAY & ALLOWANCES DOCUMENTS
|7D5K	|USE OF COUNTERFEIT PAY & ALLOWANCES DOCUMENTS
|7D5L	|USE OF COUNTERFEIT COMMISSARY DOCUMENTS
|7D5M	|USE OF COUNTERFEIT PROCUREMENT DOCUMENTS
|7D5N	|USE OF COUNTERFEIT PROPERTY DISPOSAL DOCUMENTS
|7D5P	|USE OF COUNTERFEIT NAF DOC (EXCEPT RATION CARDS)
|7E	|[SMUGGLING (OTHER THAN NARCOTICS)]
|7E1	|[SMUGGLING INTO THE UNITED STATES]
|7E1A	|SMUGGLING AMMUNITION/WEAPONS INTO THE US
|7E1B	|SMUGGLING CURRENCY INTO THE UNITED STATES
|7E1C	|SMUGGLING FIREARMS (PRIVATELY OWNED) INTO THE US
|7E1D	|SMUGGLING GOVERNMENT WEAPONS INTO THE US
|7E1E	|SMUGGLING HOSPITAL/MEDICAL SUPPLIES INTO THE US
|7E1F	|SMUGGLING LIQUOR INTO THE UNITED STATES
|7E1G	|SMUGGLING MILITARY PROPERTY INTO THE UNITED STATES
|7E1H	|SMUGGLING NAF MERCHANDISE INTO THE UNITED STATES
|7E1J	|SMUGGLING WAR TROPHIES INTO THE UNITED STATES
|7E1K	|SMUGGLING COMMISSARY ITEMS INTO THE UNITED STATES
|7E1L	|SMUGGLING PROCUREMENT ITEMS INTO THE UNITED STATES
|7E1M	|SMUGGLING PROPERTY DISPOSAL ITEMS INTO THE US
|7E2	|[SMUGGLING INTO EUROPE & BRITISH ISLES]
|7E2A	|SMUGGLING AMMUNITION/WEAPONS INTO EUROPE
|7E2A	|SMUGGLING AMMUNITION/WEAPONS INTO EUROPE
|7E2B	|SMUGGLING CURRENCY INTO EUROPE
|7E2C	|SMUGGLING FIREARMS (PRIVATELY OWNED) INTO EUROPE
|7E2D	|SMUGGLING GOVERNMENT WEAPONS INTO EUROPE
|7E2E	|SMUGGLING HOSPITAL/MEDICAL SUPPLIES INTO EUROPE
|7E2F	|SMUGGLING LIQUOR INTO EUROPE
|7E2G	|SMUGGLING MILITARY PROPERTY INTO EUROPE

|7E2H |SMUGGLING NAF MERCHANDISE INTO EUROPE
|7E2J |SMUGGLING WAR TROPHIES INTO EUROPE
|7E2K |SMUGGLING COMMISSARY ITEMS INTO EUROPE
|7E2L |SMUGGLING PROCUREMENT ITEMS INTO EUROPE
|7E2M |SMUGGLING PROPERTY DISPOSAL ITEMS INTO EUROPE
|7E3 |[SMUGGLING INTO CANADA & ALASKA]
|7E3A |SMUGGLING AMMUNITION/WEAPONS INTO CANADA
|7E3B |SMUGGLING CURRENCY INTO CANADA
|7E3C |SMUGGLING FIREARMS (PRIVATELY OWNED) INTO CANADA
|7E3D |SMUGGLING GOVERNMENT WEAPONS INTO CANADA
|7E3E |SMUGGLING HOSPITAL/MEDICAL SUPPLIES INTO CANADA
|7E3F |SMUGGLING LIQUOR INTO CANADA
|7E3G |SMUGGLING MILITARY PROPERTY INTO CANADA
|7E3H |SMUGGLING NAF MERCHANDISE INTO CANADA
|7E3H |SMUGGLING NAF MERCHANDISE INTO CANADA
|7E3J |SMUGGLING WAR TROPHIES INTO CANADA
|7E3K |SMUGGLING COMMISSARY ITEMS INTO CANADA
|7E3L |SMUGGLING PROCUREMENT ITEMS INTO CANADA
|7E3M |SMUGGLING PROPERTY DISPOSAL ITEMS INTO CANADA
|7E4 |[SMUGGLING INTO VIETNAM]
|7E4A |SMUGGLING AMMUNITION/WEAPONS INTO VIETNAM
|7E4B |SMUGGLING CURRENCY INTO VIETNAM
|7E4C |SMUGGLING FIREARMS (PRIVATELY OWNED) INTO VIETNAM
|7E4D |SMUGGLING GOVERNMENT WEAPONS INTO VIETNAM
|7E4E |SMUGGLING HOSPITAL/MEDICAL SUPPLIES INTO VIETNAM
|7E4F |SMUGGLING LIQUOR INTO VIETNAM
|7E4G |SMUGGLING MILITARY PROPERTY INTO VIETNAM
|7E4H |SMUGGLING NAF MERCHANDISE INTO VIETNAM
|7E4J |SMUGGLING WAR TROPHIES INTO VIETNAM
|7E4K |SMUGGLING COMMISSARY ITEMS INTO VIETNAM
|7E4L |SMUGGLING PROCUREMENT ITEMS INTO VIETNAM
|7E4M |SMUGGLING PROPERTY DISPOSAL ITEMS INTO VIETNAM
|7E5 |[SMUGGLING INTO KOREA]
|7E5A |SMUGGLING AMMUNITION/WEAPONS INTO KOREA
|7E5B |SMUGGLING CURRENCY INTO KOREA
|7E5B |SMUGGLING CURRENCY INTO KOREA
|7E5C |SMUGGLING FIREARMS (PRIVATELY OWNED) INTO KOREA
|7E5D |SMUGGLING GOVERNMENT WEAPONS INTO KOREA
|7E5E |SMUGGLING HOSPITAL/MEDICAL SUPPLIES INTO KOREA
|7E5F |SMUGGLING LIQUOR INTO KOREA
|7E5G |SMUGGLING MILITARY PROPERTY INTO KOREA
|7E5H |SMUGGLING NAF MERCHANDISE INTO KOREA
|7E5J |SMUGGLING WAR TROPHIES INTO KOREA
|7E5K |SMUGGLING COMMISSARY ITEMS INTO KOREA
|7E5L |SMUGGLING PROCUREMENT ITEMS INTO KOREA

|7E5M |SMUGGLING PROPERTY DISPOSAL ITEMS INTO KOREA
|7E6 |[SMUGGLING INTO THAILAND]
|7E6A |SMUGGLING AMMUNITION/WEAPONS INTO THAILAND
|7E6B |SMUGGLING CURRENCY INTO THAILAND
|7E6C |SMUGGLING FIREARMS (PRIVATELY OWNED) INTO THAILAND
|7E6D |SMUGGLING GOVERNMENT WEAPONS INTO THAILAND
|7E6E |SMUGGLING HOSPITAL/MEDICAL SUPPLIES INTO THAILAND
|7E6F |SMUGGLING LIQUOR INTO THAILAND
|7E6G |SMUGGLING MILITARY PROPERTY INTO THAILAND
|7E6H |SMUGGLING NAF MERCHANDISE INTO THAILAND
|7E6J |SMUGGLING WAR TROPHIES INTO THAILAND
|7E6J |SMUGGLING WAR TROPHIES INTO THAILAND
|7E6K |SMUGGLING COMMISSARY ITEMS INTO THAILAND
|7E6L |SMUGGLING PROCUREMENT ITEMS INTO THAILAND
|7E6M |SMUGGLING PROPERTY DISPOSAL ITEMS INTO THAILAND
|7E7 |[SMUGGLING INTO PACIFIC(NOT VIETNAM, KOREA, THAIL]
|7E7A |SMUGGLING AMMUNITION/WEAPONS INTO PACIFIC THEATER
|7E7B |SMUGGLING CURRENCY INTO PACIFIC THEATER
|7E7C |SMUGGLING FIREARMS (PRIV OWNED) INTO PACIFIC THEAT
|7E7D |SMUGGLING GOVERNMENT WEAPONS INTO PACIFIC THEATER
|7E7E |SMUGGLING HOSPITAL, MEDICAL SUPPLIES INTO PACIFIC
|7E7F |SMUGGLING LIQUOR INTO PACIFIC THEATER
|7E7G |SMUGGLING MILITARY PROPERTY INTO PACIFIC THEATER
|7E7H |SMUGGLING NAF MERCHANDISE INTO PACIFIC THEATER
|7E7J |SMUGGLING WAR TROPHIES INTO PACIFIC THEATER
|7E7K |SMUGGLING COMMISSARY ITEMS INTO PACIFIC THEATER
|7E7L |SMUGGLING PROCUREMENT ITEMS INTO PACIFIC THEATER
|7E7M |SMUGGLING PROPERTY DISPOSAL ITEMS INTO PACIFIC
|7E8 |[SMUGGLING INTO SOUTH AMERICA & CARIBBEAN]
|7E8A |SMUGGLING AMMUNITION/WEAPONS INTO SOUTH AMERICA
|7E8B |SMUGGLING CURRENCY INTO SOUTH AMERICA
|7E8C |SMUGGLING FIREARMS (PRIV OWNED) INTO SOUTH AMERICA
|7E8C |SMUGGLING FIREARMS (PRIV OWNED) INTO SOUTH AMERICA
|7E8D |SMUGGLING GOVERNMENT WEAPONS INTO SOUTH AMERICA
|7E8E |SMUGGLING HOSPITAL/MEDICAL SUPPLIES INTO SO AMER
|7E8F |SMUGGLING LIQUOR INTO SOUTH AMERICA
|7E8G |SMUGGLING MILITARY PROPERTY INTO SOUTH AMERICA
|7E8H |SMUGGLING NAF MERCHANDISE INTO SOUTH AMERICA
|7E8J |SMUGGLING WAR TROPHIES INTO SOUTH AMERICA

|7E8K |SMUGGLING COMMISSARY ITEMS INTO SOUTH AMERICA
|7E8L |SMUGGLING PROCUREMENT ITEMS INTO SOUTH AMERICA
|7E8M |SMUGGLING PROPERTY DISPOSAL ITEMS INTO SO AMERICA
|7E9 |[SMUGGLING INTO OTHER COUNTRIES]
|7E9A |SMUGGLING AMMUNITION/WEAPONS INTO OTHER COUNTRIES
|7E9B |SMUGGLING CURRENCY INTO OTHER COUNTRIES
|7E9C |SMUGGLING FIREARMS (PRIV OWNED) INTO OTR COUNTRIES
|7E9D |SMUGGLING GOVERNMENT WEAPONS INTO OTHER COUNTRIES
|7E9E |SMUGGLING HOSPITAL/MEDICAL SUPPLIES INTO OTR COUNT
|7E9F |SMUGGLING LIQUOR INTO OTHER COUNTRIES
|7E9G |SMUGGLING MILITARY PROPERTY INTO OTHER COUNTRIES
|7E9H |SMUGGLING NAF MERCHANDISE INTO OTHER COUNTRIES
|7E9J |SMUGGLING WAR TROPHIES INTO OTHER COUNTRIES
|7E9K |SMUGGLING COMMISSARY ITEMS INTO OTHER COUNTRIES
|7E9K |SMUGGLING COMMISSARY ITEMS INTO OTHER COUNTRIES
|7E9L |SMUGGLING PROCUREMENT ITEMS INTO OTHER COUNTRIES
|7E9M |SMUGGLING PROPERTY DISPOSAL ITEMS INTO OTR COUNTRI
|7F |[LARCENY OF GOVERNMENT PROPERTY]
|7F1 |[LARCENY OF GOVT PROPERTY, (NOT FUNDS OR WEAPONS)]
|7F1A |[LARCENY OF GP, NOT POL/FUNDS/WEAPONS/PROP DISP/]
|7F1A1 |LARCENY OF GOVERNMENT PROPERTY, $50 & OVER
|7F1A2 |LARCENY OF GOVERNMENT PROPERTY, UNDER $50
|7F1A3 |LARCENY OF MILT PROPERTY $100 OR LESS
|7F1A4 |LARCENY OF MILT PROPERTY MORE THAN $100
|7F1B |[LARCENY OF PROPERTY DISPOSAL PROPERTY]
|7F1B1 |LARCENY OF PROPERTY DISPOSAL PROPERTY, $50 & OVER
|7F1B2 |LARCENY OF PROPERTY DISPOSAL PROPERTY, UNDER $50
|7F1C |[LARCENY OF GOVERNMENT PROPERTY, PROCUREMENT]
|7F1C1 |LARCENY OF GOVT PROPERTY, PROCUREMENT, $50 & OVER
|7F1C2 |LARCENY OF GOVT PROPERTY, PROCUREMENT, UNDER $50
|7F1D |[LARCENY OF GOVERNMENT PROPERTY, POL ITEMS]
|7F1D1 |LARCENY OF GOVERNMENT PROPERTY, POL, $50 & OVER
|7F1D2 |LARCENY OF GOVERNMENT PROPERTY, POL, UNDER $50
|7F1E |[LARCENY OF GOVERNMENT PROPERTY, COMMISSARY ITEMS]

|7F1E1 |LARCENY OF GOVT PROPERTY, COMMISSARY, $50 & OVER
|7F1E2 |LARCENY OF GOVT PROPERTY, COMMISSARY UNDER $50
|7F1F |LARCENY OF COMPUTER TIME
|7F1F |LARCENY OF COMPUTER TIME
|7F1G |LARCENY INVOLVING USE OF A COMPUTER (SUPPL CODE)
|7F2 |[LARCENY OF GOVERNMENT FUNDS]
|7F2A |[LARCENY OF GOVT FUNDS NOT CHECK, POL/PROP DI]
|7F2A1 |LARCENY OF GOVERNMENT FUNDS, $50 & OVER
|7F2A2 |LARCENY OF GOVERNMENT FUNDS, UNDER $50
|7F2B |[LARCENY OF GOV CHECK, NOT POL/ PROP DISP/PROCURE]
|7F2B1 |LARCENY OF GOVERNMENT CHECK, $50 & OVER
|7F2B2 |LARCENY OF GOVERNMENT CHECK, UNDER $50
|7F2C |[LARCENY OF PROPERTY DISPOSAL FUNDS]
|7F2C1 |LARCENY OF PROPERTY DISPOSAL FUNDS, $50 & OVER
|7F2C2 |LARCENY OF PROPERTY DISPOSAL FUNDS, UNDER $50
|7F2C3 |LARCENY OF PROPERTY DISPOSAL CHECK, $50 & OVER
|7F2C4 |LARCENY OF PROPERTY DISPOSAL CHECK, UNDER $50
|7F2D |[LARCENY OF GOVERNMENT PROCUREMENT FUNDS]
|7F2D1 |LARCENY OF GOVT PROCUREMENT FUNDS, $50 & OVER
|7F2D2 |LARCENY OF GOVERNMENT PROCUREMENT FUNDS, UNDER $50
|7F2D3 |LARCENY OF GOVT PROCUREMENT CHECK, $50 & OVER
|7F2D4 |LARCENY OF GOVERNMENT PROCUREMENT CHECK, UNDER $50
|7F2E |[LARCENY OF GOVERNMENT POL FUNDS]
|7F2E1 |LARCENY OF GOVERNMENT POL FUNDS, $50 & OVER
|7F2E1 |LARCENY OF GOVERNMENT POL FUNDS, $50 & OVER
|7F2E2 |LARCENY OF GOVERNMENT POL FUNDS, UNDER $50
|7F2E3 |LARCENY OF GOVERNMENT POL CHECK, $50 & OVER
|7F2E4 |LARCENY OF GOVERNMENT POL CHECK, UNDER $50
|7F2F |[LARCENY OF GOVERNMENT COMMISSARY FUNDS]
|7F2F1 |LARCENY OF GOVERNMENT COMMISSARY FUNDS, $50 & OVER
|7F2F2 |LARCENY OF GOVERNMENT COMMISSARY FUNDS, UNDER $50
|7F2F3 |LARCENY OF GOVERNMENT COMMISSARY CHECK, $50 & OVER
|7F2F4 |LARCENY OF GOVERNMENT COMMISSARY CHECK, UNDER $50
|7F2G |LARCENY OF GOVT FUNDS INVOLVING USE OF A COMPUTER
|7F3 |[WRONGFUL APPROPRIATION OF GOVERNMENT PROPERTY]
|7F3A |[WRONGFUL APPROP OF GOVT PROPERTY, NOT PROCUREMENT

|7F3A1 |WRONGFUL APPROP OF GOVERNMENT PROPERTY, $50 & OVER
|7F3A2 |WRONGFUL APPROP OF GOVERNMENT PROPERTY, UNDER $50
|7F3A3 |MISAPPROPRIATE: MILT PROPERTY $100 OR LESS
|7F3A4 |MISAPPROPRIATE: MILT PROPERTY MORE THAN $100
|7F3A5 |MISAPPROPRIATE: MILT VEHICLE, BOAT, AIRCRAFT
|7F3B |[WRONGFUL APPROP OF PROPERTY DISPOSAL PROPERTY]
|7F3B1 |WRONGFUL APPROP OF PROPERTY DISPOSAL PROPERTY,+$50
|7F3B2 |WRONGFUL APPROP OF PROPERTY DISPOSAL PROPERTY,-$50
|7F3C |[WRONGFUL APPROP OF GOVT PROCUREMENT PROPERTY]
|7F3C1 |WRONGFUL APPROP OF GOVT PROCURE PROPERTY, $50 & +
|7F3C2 |WRONGFUL APPROP OF GOVT PROCUREMENT PROPERTY, $50
|7F3D |[WRONGFUL APPROPRIATION OF GOVERNMENT VEHICLE]
|7F3D |[WRONGFUL APPROPRIATION OF GOVERNMENT VEHICLE]
|7F3D1 |WRONGFUL APPROP OF GOVERNMENT VEHICLE, $50 & OVER
|7F3D2 |WRONGFUL APPROPR OF GOVERNMENT VEHICLE, UNDER $50
|7F3E |[WRONGFUL APPROPRIATION OF GOVERNMENT POL ITEMS]
|7F3E1 |WRONGFUL APPROP OF GOVERNMENT POL, $50 & OVER
|7F3E2 |WRONGFUL APPROP OF GOVERNMENT POL, UNDER $50
|7F3F |[WRONGFUL APPROP OF GOVT COMMISSARY PROPERTY]
|7F3F1 |WRONGFUL APPROP OF GOVT COMMISSARY PROPERTY, $50+
|7F3F2 |WRONGFUL APPROP OF GOVT COMMISSARY PROPERTY, -$50
|7F3G |WRONGFUL APPROP OF GOVT PROPERTY USING A COMPUTER
|7F3H |[WRONGFUL APPROPRIATION OF ACTIVE ARMY AIRCRAFT]
|7F3H1 |WRONGFUL APPROP OF ACTIVE ARMY AIRCRAFT, ON POST
|7F3H2 |WRONGFUL APPROP OF ACTIVE ARMY AIRCRAFT, OFF POST
|7F3H3 |WRONGFUL APPROP OF ACTIVE ARMY AIRCRAFT,FIXED WING
|7F3H4 |WRONGFUL APPROP OF ACTIVE ARMY AIRCRAFT, ROTARY
|7F3H5 |WRONGFUL APPROP OF ACTIVE ARMY AIRCRAFT COMPONENTS
|7F3J |[WRONGFUL APPROP OF NATIONAL GUARD AIRCRAFT]
|7F3J1 |WRONGFUL APPROP OF NATIONAL GUARD AIRCRAFT,ON

	POST
|7F3J2	|WRONGFUL APPROP OF NG AIRCRAFT, OFF POST
|7F3J3	|WRONGFUL APPROP OF NG AIRCRAFT, FIXED WING
|7F3J4	|WRONGFUL APPROP OF NATIONAL GUARD AIRCRAFT, ROTARY
|7F3J4	|WRONGFUL APPROP OF NATIONAL GUARD AIRCRAFT, ROTARY
|7F3J5	|WRONGFUL APPROP OF NG AIRCRAFT COMPONENTS
|7F3K	|[WRONGFUL APPROPRIATION OF ARMY RESERVE AIRCRAFT]
|7F3K1	|WRONGFUL APPROP OF ARMY RESERVE AIRCRAFT, ON POST
|7F3K2	|WRONGFUL APPROP OF ARMY RESERVE AIRCRAFT, OFF POST
|7F3K3	|WRONGFUL APPROP OF RESERVE AIRCRAFT, FIXED WING
|7F3K4	|WRONGFUL APPROP OF ARMY RESERVE AIRCRAFT, ROTARY
|7F3K5	|WRONGFUL APPROP OF RESERVE AIRCRAFT COMPONENTS
|7F3L	|[WRONGFUL APPROPRIATION OF ACTIVE ARMY VEHICLES]
|7F3L1	|WRONGFUL APPROP OF ACTIVE ARMY VEHICLES, ON POST
|7F3L2	|WRONGFUL APPROP OF ACTIVE ARMY VEHICLES, OFF POST
|7F3L3	|WRONGFUL APPROP OF ARMY TACTICAL WHEELED VEHICLES
|7F3L4	|WRONGFUL APPROP OF ARMY TACTICAL TRACKED VEHICLES
|7F3L5	|WRONGFUL APPROP OF ACTIVE ARMY VEHICLE COMPONENTS
|7F3L6	|WRONGFUL APPROP OF ACTIVE ARMY COMMERCIAL VEHICLES
|7F3M	|[WRONGFUL APPROP OF NATIONAL GUARD VEHICLES]
|7F3M1	|WRONGFUL APPROP OF NG VEHICLES, ON POST
|7F3M2	|WRONGFUL APPROP OF NG VEHICLES, OFF POST
|7F3M3	|WRONGFUL APPROP OF NG TACTICAL WHEELED VEHICLES
|7F3M4	|WRONGFUL APPROP OF NG TACTICAL TRACKED VEHICLES
|7F3M5	|WRONGFUL APPROP OF NG VEHICLE COMPONENTS
|7F3M5	|WRONGFUL APPROP OF NG VEHICLE COMPONENTS
|7F3M6	|WRONGFUL APPROP OF NG COMMERCIAL VEHICLES
|7F3N	|[WRONGFUL APPROPRIATION OF ARMY RESERVE VEHICLES]
|7F3N1	|WRONGFUL APPROP OF ARMY RESERVE VEHICLES, ON POST
|7F3N2	|WRONGFUL APPROP OF ARMY RESERVE VEHICLES, OFF POST

|7F3N3 |WRONGFUL APPROP OF RESERVE TACTICAL WHEELED VEH
|7F3N4 |WRONGFUL APPROP OF RESERVE TACTICAL TRACKED VEH
|7F3N5 |WRONGFUL APPROP OF ARMY RESERVE VEHICLE COMPONENTS
|7F3N6 |WRONGFUL APPROP OF RESERVE COMMERCIAL VEHICLES
|7F4 |[WRONGFUL DISPOSITION OF GOVERNMENT PROPERTY]
|7F4A |[WRONGFUL DISPOSITION OF GOVT PROPERTY NOT PROCUR]
|7F4A1 |WRONGFUL DISPOSITION OF GOVT PROPERTY, $50 & OVER
|7F4A2 |WRONGFUL DISPOSITION OF GOVT PROPERTY, UNDER $50
|7F4B |[WRONGFUL DISPO OF PROPERTY DISPOSAL PROPERTY]
|7F4B1 |WRONGFUL DISPO OF PROPERTY DISPOSAL PROPERTY, $50+
|7F4B2 |WRONGFUL DISPO OF PROPERTY DISPOSAL PROPERTY, -$50
|7F4C |[WRONGFUL DISPO OF GOVT PROCUREMENT PROPERTY]
|7F4C1 |WRONGFUL DISPO OF GOVT PROCUREMENT PROPERTY, $50+
|7F4C2 |WRONGFUL DISPO OF GOVT PROCUREMENT PROPERTY -$50
|7F4D |[WRONGFUL DISPOSITION OF GOVERNMENT POL ITEMS]
|7F4D1 |WRONGFUL DISPOSITION OF GOVERNMENT POL, $50 & OVER
|7F4D1 |WRONGFUL DISPOSITION OF GOVERNMENT POL, $50 & OVER
|7F4D2 |WRONGFUL DISPOSITION OF GOVERNMENT POL, UNDER $50
|7F4E |[WRONGFUL DISPOSITION OF COMMISSARY PROPERTY]
|7F4E1 |WRONGFUL DISPO OF COMMISSARY PROPERTY, $50 & OVER
|7F4E2 |WRONGFUL DISPO OF COMMISSARY PROPERTY, UNDER $50
|7F4F |[WRONGFUL DISPOSITION OF GOVERNMENT VEHICLE]
|7F4F1 |WRONGFUL DISPOSITION OF GOVT VEHICLE, $50 OR OVER
|7F4F2 |WRONGFUL DISPOSITION OF GOVT VEHICLE, UNDER $50
|7F4G |WRONGFUL DISPO OF GOVT PROPERTY USING A COMPUTER
|7F4H1 |SELL MILT PROPERTY: 100 OR LESS
|7F4H2 |SELL MILT PROPERTY: MORE THAN $100
|7F4H3 |SELL MILT PROPERTY: FIREARM OR EXPLOSIVE
|7F5 |[LARCENY OF NAF PROPERTY]
|7F5A |[LARCENY OF NAF PROPERTY OTR THAN POL & NOT AAFES]
|7F5A1 |LARCENY OF NAF PROPERTY, $50 & OVER

|7F5A2 |LARCENY OF NAF PROPERTY, UNDER $50
|7F5B |[LARCENY OF AAFES PROPERTY (NOT INCLUDING POL]
|7F5B1 |LARCENY OF AAFES PROPERTY, $50 & OVER
|7F5B2 |LARCENY OF AAFES PROPERTY, UNDER $50
|7F5C |[LARCENY OF NAF PROPERTY, POL ITEMS]
|7F5C1 |LARCENY OF NAF PROPERTY, POL, $50 & OVER
|7F5C2 |LARCENY OF NAF PROPERTY, POL, UNDER $50
|7F5D |LARCENY OF NAF PROPERTY, INVL USE OF A COMPUTER
|7F5E |[LARCENY OF NONAPPROPRIATED FUNDS]
|7F5E |[LARCENY OF NONAPPROPRIATED FUNDS]
|7F5E1 |LARCENY OF NONAPPROPRIATED FUNDS, $50 & OVER
|7F5E2 |LARCENY OF NONAPPROPRIATED FUNDS, UNDER $50
|7F5E3 |LARCENY OF NAF BY CHECK, $50 & OVER
|7F5E4 |LARCENY OF NAF BY CHECK, UNDER $50
|7F5E5 |LARCENY OF AAFES FUNDS, $50 & OVER
|7F5E6 |LARCENY OF AAFES FUNDS, UNDER $50
|7F5E7 |LARCENY OF AAFES FUNDS BY CHECK, $50 & OVER
|7F5E8 |LARCENY OF AAFES FUNDS BY CHECK, UNDER $50
|7F5F |LARCENY OF NAF PROPERTY INVOLVING USE OF COMPUTER
|7F6 |[WRONGFUL APPROPRIATION OF NAF FUND PROPERTY]
|7F6A |[WRONGFUL APPROP OF NAF FUND PROPERTY NOT POL]
|7F6A1 |WRONGFUL APPROPRIATION OF NAF PROPERTY,$50 OR OVER
|7F6A2 |WRONGFUL APPROPRIATION OF NAF PROPERTY, UNDER $50
|7F6B |[WRONGFUL APPROPRIATION OF AAFES PROPERTY,NOT POL]
|7F6B1 |WRONGFUL APPROP OF AAFES PROPERTY, $50 OR OVER
|7F6B2 |WRONGFUL APPROPRIATION OF AAFES PROPERTY,UNDER $50
|7F6C |[WRONGFUL APPROPRIATION OF NAF POL ITEMS]
|7F6C1 |WRONGFUL APPROPRIATION OF NAF POL, $50 & OVER
|7F6C2 |WRONGFUL APPROPRIATION OF NAF POL, UNDER $50
|7F6D |WRONGFUL APPROP OF NAF PROPERTY USING A COMPUTER
|7F6D |WRONGFUL APPROP OF NAF PROPERTY USING A COMPUTER
|7F7 |[WRONGFUL DISPOSITION OF NAF PROPERTY]
|7F7A |[WRONGFUL DISPOSITION OF NAF PROPERTY, NOT POL]
|7F7A1 |WRONGFUL DISPOSITION OF NAF PROPERTY, $50 & OVER
|7F7A2 |WRONGFUL DISPOSITION OF NAF PROPERTY, UNDER $50
|7F7B |[WRONGFUL DISPOSITION OF AAFES PROPERTY (NOT POL]
|7F7B1 |WRONGFUL DISPOSITION OF AAFES PROPERTY, $50 & OVER
|7F7B2 |WRONGFUL DISPOSITION OF AAFES PROPERTY, UNDER

$50
|7F7C |[WRONGFUL DISPOSITION OF NAF POL ITEMS]
|7F7C1 |WRONGFUL DISPOSITION OF NAF POL ITEMS, UNDER $50
|7F7C2 |WRONGFUL DISPOSITION OF NAF POL ITEMS, $50 & OVER
|7F7D |WRONGFUL DISPOSITION OF NAF PROPERTY BY COMPUTER
|7F8 |[LARCENY OF GOVERNMENT WEAPONS/MUNITIONS]
|7F8A |[LARCENY OF GOVERNMENT WEAPONS]
|7F8A1 |LARCENY OF GOVERNMENT WEAPONS, $50 & OVER
|7F8A2 |LARCENY OF GOVERNMENT WEAPONS, UNDER $50
|7F8A3 |LARCENY OF GOVERNMENT WEAPONS USING A COMPUTER
|7F8B |[LARCENY OF GOVERNMENT MUNITIONS]
|7F8B1 |LARCENY OF GOVERNMENT MUNITIONS, $50 & OVER
|7F8B2 |LARCENY OF GOVERNMENT MUNITIONS, UNDER $50
|7F8B3 |LARCENY OF GOVERNMENT MUNITIONS USING A COMPUTER
|7F8B3 |LARCENY OF GOVERNMENT MUNITIONS USING A COMPUTER
|7F8C |[LARCENY OF GOVERNMENT WEAPONS/MUNITIONS PARTS]
|7F8C1 |LARCENY OF GOVT WEAPONS/MUNITIONS PARTS $50 & OVER
|7F8C2 |LARCENY OF GOVT WEAPONS/MUNITIONS PARTS, UNDER $50
|7F8C3 |LARCENY OF GOVT WEAPONS/MUNITIONS USING A COMPUTER
|7F9 |[LARCENY OF GOVERNMENT MOTOR VEHICLES]
|7F9A |LARCENY OF GOVERNMENT MOTOR VEHICLES, $50 & OVER
|7F9B |LARCENY OF GOVERNMENT MOTOR VEHICLES, UNDER $50
|7F9C |LARCENY OF GOVT MOTOR VEHICLES USING A COMPUTER
|7F9D |[LARCENY OF ACTIVE ARMY AIRCRAFT]
|7F9D1 |LARCENY OF ACTIVE ARMY AIRCRAFT, ON POST
|7F9D2 |LARCENY OF ACTIVE ARMY AIRCRAFT, OFF POST
|7F9D3 |LARCENY OF ACTIVE ARMY AIRCRAFT, FIXED WING
|7F9D4 |LARCENY OF ACTIVE ARMY AIRCRAFT, ROTARY
|7F9D5 |LARCENY OF ACTIVE ARMY AIRCRAFT COMPONENTS
|7F9E |[LARCENY OF NATIONAL GUARD AIRCRAFT]
|7F9E1 |LARCENY OF NATIONAL GUARD AIRCRAFT, ON POST
|7F9E2 |LARCENY OF NATIONAL GUARD AIRCRAFT, OFF POST
|7F9E3 |LARCENY OF NATIONAL GUARD AIRCRAFT, FIXED WING
|7F9E4 |LARCENY OF NATIONAL GUARD AIRCRAFT, ROTARY
|7F9E5 |LARCENY OF NATIONAL GUARD AIRCRAFT COMPONENTS
|7F9E5 |LARCENY OF NATIONAL GUARD AIRCRAFT COMPONENTS
|7F9F |[LARCENY OF ARMY RESERVE AIRCRAFT]
|7F9F1 |LARCENY OF ARMY RESERVE AIRCRAFT, ON POST
|7F9F2 |LARCENY OF ARMY RESERVE AIRCRAFT, OFF POST

|7F9F3 |LARCENY OF ARMY RESERVE AIRCRAFT, FIXED WING
|7F9F4 |LARCENY OF ARMY RESERVE AIRCRAFT, ROTARY
|7F9F5 |LARCENY OF ARMY RESERVE AIRCRAFT, COMPONENTS
|7F9G |[LARCENY OF ACTIVE ARMY VEHICLE]
|7F9G1 |LARCENY OF ACTIVE ARMY VEHICLE, ON POST
|7F9G2 |LARCENY OF ACTIVE ARMY VEHICLE, OFF POST
|7F9G3 |LARCENY OF ACTIVE ARMY TACTICAL WHEELED VEHICLE
|7F9G4 |LARCENY OF ACTIVE ARMY TACTICAL TRACKED VEHICLE
|7F9G5 |LARCENY OF ACTIVE ARMY VEHICLE COMPONENTS
|7F9G6 |LARCENY OF ACTIVE ARMY COMMERCIAL VEHICLE
|7F9H |[LARCENY OF NATIONAL GUARD VEHICLE]
|7F9H1 |LARCENY OF NATIONAL GUARD VEHICLE, ON POST
|7F9H2 |LARCENY OF NATIONAL GUARD VEHICLE, OFF POST
|7F9H3 |LARCENY OF NATIONAL GUARD TACTICAL WHEELED VEHICLE
|7F9H4 |LARCENY OF NATIONAL GUARD TACTICAL TRACKED VEHICLE
|7F9H5 |LARCENY OF NATIONAL GUARD VEHICLE COMPONENTS
|7F9H6 |LARCENY OF NATIONAL GUARD COMMERCIAL VEHICLE
|7F9H6 |LARCENY OF NATIONAL GUARD COMMERCIAL VEHICLE
|7F9J |[LARCENY OF ARMY RESERVE VEHICLE]
|7F9J1 |LARCENY OF ARMY RESERVE VEHICLE, ON POST
|7F9J2 |LARCENY OF ARMY RESERVE VEHICLE, OFF POST
|7F9J3 |LARCENY OF ARMY RESERVE TACTICAL WHEELED VEHICLE
|7F9J4 |LARCENY OF ARMY RESERVE TACTICAL TRACKED VEHICLE
|7F9J5 |LARCENY OF ARMY RESERVE VEHICLE COMPONENTS
|7F9J6 |LARCENY OF ARMY RESERVE COMMERCIAL VEHICLE
|7G |[LARCENY OF PRIVATE PROPERTY/FUNDS]
|7G1 |[LARCENY OF PRIVATE PROPERTY]
|7G1A |[LARCENY OF PVT PROP NOT POL/FUNDS/AUTOS/BILLETS]
|7G1A1 |LARCENY OF PRIVATE PROPERTY, $50 & OVER
|7G1A2 |LARCENY OF PRIVATE PROPERTY, UNDER $50
|7G1A3 |LARCENY: NONMILT PROPERTY $100 OR LESS
|7G1A3 |LARCENY: NONMILT PROPERTY MORE THAN $100
|7G1B |[LARCENY OF PVT PROP FROM TRP BILLETS, NOT FUNDS]
|7G1B1 |LARCENY OF PVT PROP FROM TROOP BILLETS, $50 & OVER
|7G1B2 |LARCENY OF PVT PROP FROM TROOP BILLETS, UNDER $50
|7G1C |[LARCENY OF PRIVATE PROPERTY, POL ITEMS]
|7G1C1 |LARCENY OF PRIVATE PROP, POL ITEMS, $50 OR OVER
|7G1C2 |LARCENY OF PRIVATE PROPERTY, POL ITEMS, UNDER $50
|7G1D |LARCENY OF PRIVATE PROPERTY, USING A COMPUTER
|7G2 |[LARCENY OF PRIVATE FUNDS]
|7G2 |[LARCENY OF PRIVATE FUNDS]
|7G2A |[LARCENY OF PVT FUNDS NOT CHECKS OR FROM BILLETS]
|7G2A1 |LARCENY OF PRIVATE FUNDS, $50 & OVER

|7G2A2 |LARCENY OF PRIVATE FUNDS, UNDER $50
|7G2B |[LARCENY OF PVT FUNDS NOT CHECKS/FROM TRP BILLETS]
|7G2B1 |LARCENY OF PVT FUNDS FROM TRP BILLETS, $50 & OVER
|7G2B2 |LARCENY OF PVT FUNDS FROM TRP BILLETS, UNDER $50
|7G2C |LARCENY OF PVT FUNDS FROM TRP BILLETS, BY COMPUTER
|7G3 |[LARCENY OF PRIVATE MOTOR VEHICLE]
|7G3A |LARCENY OF PVT VEHICLE BOAT OR AIRCRAFT, $50 & OVR
|7G3B |LARCENY OF PVT VEHICLE BOAT OR AIRCRAFT, UNDER $50
|7G3C |LARCENY OF PVT MOTORCYCLE, SCOOTER, ETC, OVER $50
|7G3D |LARCENY OF PVT MOTORCYCLE, SCOOTER, ETC, UNDER $50
|7G3E |LARCENY OF PVT MOTOR VEHICLE USING A COMPUTER
|7G4 |[LARCENY OF PRIVATE FUNDS BY MEANS OF CHECK]
|7G4A |LARCENY OF PVT FUNDS BY MEANS OF CHECK, $50 & OVER
|7G4B |LARCENY OF PVT FUNDS BY MEANS OF CHECK, UNDER $50
|7G4C |LARCENY OF PVT FUNDS BY CHECK USING A COMPUTER
|7G5 |[WRONGFUL APPROPRIATION OF PRIVATE PROPERTY]
|7G5A |[WRONGFUL APPROPRIATION OF PVT PROP NOT POL ITEMS]
|7G5A1 |WRONGFUL APPROPRIATION OF PVT PROPERTY, $50 & OVER
|7G5A2 |WRONGFUL APPROPRIATION OF PVT PROPERTY, UNDER $50
|7G5A3 |MISAPPROPRIATE: NONMILT PROPERTY $100 OR LESS
|7G5A4 |MISAPPROPRIATE: NOMMILT PROPERTY MORE THAN $100
|7G5A5 |MISAPPROPRIATE: NOMMILT VEHICLE, BOAT, AIRCRAFT
|7G5B |[WRONGFUL APPROP OF PVT PROP FROM TRP BILLETS]
|7G5B1 |WRONGFUL APPROP OF PVT PROP FROM TRP BILL, OVR $50
|7G5B2 |WRONGFUL APPROP OF PVT PROP FROM TRP BILL, UDR $50
|7G5C |[WRONGFUL APPROPRIATION OF PVT PROP, POL ITEMS]
|7G5C1 |WRONGFUL APPROP OF PVT PROP, POL ITEMS, $50 & OVER
|7G5C2 |WRONGFUL APPROP OF PVT PROP, POL ITEMS, UNDER $50
|7G5D |WRONGFUL APPROPRIATION OF PVT PROP WITH A COMPUTER
|7G6 |[WRONGFUL APPROPRIATION OF PRIVATE MOTOR VEHICLE]
|7G6A |WRONGFUL APPROP OF PVT VEH, BOAT OR AIRCRAFT, >$50
|7G6B |WRONGFUL APPROP OF PVT VEH, BOAT OR AIRCRAFT, <$50

|7G6C |WRONGFUL APPROP OF PVT MC, SCOOTER, ETC OVER $50
|7G6D |WRONGFUL APPROP OF PVT MC, SCOOTER, ETC UNDER $50
|7G6E |WRONGFUL APPROP OF PVT PROP USING A COMPUTER
|7G7 |[WRONGFUL DISPOSITION OF PRIVATE PROPERTY]
|7G7A |[WRONGFUL DISPO OF PVT PROP NOT FROM TRP BILLETS]
|7G7A1 |WRONGFUL DISPOSITION OF PVT PROPERTY, $50 & OVER
|7G7A2 |WRONGFUL DISPOSITION OF PVT PROPERTY, UNDER $50
|7G7B |[WRONGFUL DISPOSITION OF PVT PROP FRM TRP BILLETS]
|7G7B1 |WRONGFUL DISPO OF PVT PROP FROM TRP BILL, OVER $50
|7G7B1 |WRONGFUL DISPO OF PVT PROP FROM TRP BILL, OVER $50
|7G7B2 |WRONGFUL DISP OF PVT PROP FROM TRP BILL, UNDER $50
|7G7C |WRONGFUL DISPOSITION OF PVT PROP USING A COMPUTER
|7H |[POSTAL VIOLATIONS]
|7H1 |LARCENY OF OR FROM THE U.S. MAIL
|7H2 |OBSTRUCTING OR SECRETING U.S. MAIL
|7H3 |DESTRUCTION OF U.S. MAIL
|7H4 |DEPOSITING PROHIBITED MATTER IN U.S. MAIL
|7H5 |OTHER POSTAL VIOLATIONS
|7H6 |[MAIL FRAUDS (18 USC)]
|7H6A |OTHER POSTAL VIOLATIONS (NOT 7H6B - 7H6H)
|7H6B |MAIL FRAUDS OF A FINANCE ACTIVITY
|7H6C |MAIL FRAUDS OF A PERSONNEL ACTIVITY
|7H6D |MAIL FRAUDS OF A COMMISSARY ACTIVITY
|7H6E |MAIL FRAUDS OF A PROCUREMENT ACTIVITY
|7H6F |MAIL FRAUDS OF A AAFES ACTIVITY
|7H6G |MAIL FRAUDS OF A NAF INSTRUMENTALITY
|7H6H |MAIL FRAUDS OF A PROPERTY DISPOSAL ACTIVITY
|7H7 |MAIL: DESTROY, STEAL/TAKE/OPEN
|7H8 |MAIL: DEPOSIT OBSCENITY
|7H9 |MAIL: ALL OTHER
|7J |[WRONGFUL DESTRUCTION]
|7J1 |[WRGFUL DEST OF GVT PROP NOT PAY DOCS/COMM PROP)]
|7J1A |WRONGFUL DEST OF ACTIVE ARMY AIRCRAFT (ON POST)
|7J1A |WRONGFUL DEST OF ACTIVE ARMY AIRCRAFT (ON POST)
|7J1A1 |WRONGFUL DEST OF ACTIVE ARMY AIRCRAFT (OFF POST)
|7J1A2 |WRONGFUL DEST OF ACTIVE ARMY FIXED WING AIRCRAFT
|7J1A3 |WRONGFUL DEST OF ACTIVE ARMY ROTARY AIRCRAFT
|7J1A4 |WRONGFUL DEST OF ACTIVE ARMY AIRCRAFT COMPONENTS
|7J1B |WRONGFUL DEST OF NAT GUARD AIRCRAFT (ON POST)
|7J1B1 |WRONGFUL DEST OF NAT GUARD AIRCRAFT (OFF POST)
|7J1B2 |WRONGFUL DEST OF NAT GUARD FIXED WING AIRCRAFT
|7J1B3 |WRONGFUL DEST OF NAT GUARD ROTARY AIRCRAFT

|7J1B4 |WRONGFUL DEST OF NAT GUARD AIRCRAFT COMPONENTS
|7J1C |WRONGFUL DEST OF ARMY RESERVE AIRCRAFT (ON POST)
|7J1C1 |WRONGFUL DEST OF ARMY RESERVE AIRCRAFT (OFF POST)
|7J1C2 |WRONGFUL DEST OF ARMY RESERVE FIXED WING AIRCRAFT
|7J1C3 |WRONGFUL DEST OF ARMY RESERVE ROTARY AIRCRAFT
|7J1C4 |WRONGFUL DEST OF ARMY RESERVE AIRCRAFT COMPONENTS
|7J1D |WRONGFUL DEST OF ACTIVE ARMY VEHICLE (ON POST)
|7J1D1 |WRONGFUL DEST OF ACTIVE ARMY VEHICLE (OFF POST)
|7J1D2 |WRONGFUL DEST OF ACTIVE ARMY TACTICAL WHEELED VEH
|7J1D3 |WRONGFUL DEST OF ACTIVE ARMY TACTICAL TRACKED VEH
|7J1D4 |WRONGFUL DEST OF ACTIVE ARMY COMMERCIAL VEHICLE
|7J1D5 |WRONGFUL DEST OF ACTIVE ARMY VEHICLE COMPONENTS
|7J1D5 |WRONGFUL DEST OF ACTIVE ARMY VEHICLE COMPONENTS
|7J1E |WRONGFUL DEST OF NATIONAL GUARD VEHICLE (ON POST)
|7J1E1 |WRONGFUL DEST OF NATIONAL GUARD VEHICLE (OFF POST)
|7J1E2 |WRONGFUL DEST OF NAT GUARD TACTICAL WHEELED VEH
|7J1E3 |WRONGFUL DEST OF NAT GUARD TACTICAL TRACKED VEH
|7J1E4 |WRONGFUL DEST OF NAT GUARD COMMERCIAL VEHICLE
|7J1E5 |WRONGFUL DEST OF NAT GUARD VEHICLE COMPONENTS
|7J1F |WRONGFUL DEST OF ARMY RESERVE VEHICLE (ON POST)
|7J1F1 |WRONGFUL DEST OF ARMY RESERVE VEHICLE (OFF POST)
|7J1F2 |WRONGFUL DEST OF ARMY RESERVE TACTICAL WHEELED VEH
|7J1F3 |WRONGFUL DEST OF ARMY RESERVE TACTICAL TRACKED VEH
|7J1F4 |WRONGFUL DEST OF ARMY RESERVE VEHICLE COMPONENTS
|7J1F5 |WRONGFUL DEST OF ARMY RESERVE COMMERCIAL VEHICLE
|7J2 |WRONGFUL DAMAGING OF GOVT PROPERTY, NOT COMMISSARY
|7J2A1 |NEGLECT: DAMAGE MILT PROPERTY: $100 OR LESS
|7J2A2 |NEGLECT: DAMAGE MILT PROPERTY: MORE THAN $100
|7J2B1 |WILFUL: DAMAGE MILT PROPERTY: $100 OR LESS
|7J2B2 |WILFUL: DAMAGE MILT PROPERTY: MORE THAN $100
|7J2B3 |WILFUL: DAMAGE MILT PROPERTY: FIREARMS OR EXPLOSIV

|7J2C1 |HAZARD VESSEL: WILLFUL
|7J2C2 |HAZARD VESSEL: NEGLECT
|7J3 |LOSS OF GOVERNMENT PROPERTY THROUGH NEGLECT
|7J4 |WRONGFUL DESTRUCTION OF PRIVATE PROPERTY
|7J5 |WRONGFUL DAMAGING OF PRIVATE PROPERTY
|7J5A1 |WASTE OR SPOIL NONMILT PROPERTY: $100 OR LESS
|7J5A2 |WASTE OR SPOIL NONMILT PROPERTY: MORE THAN $100
|7J5B1 |DESTROY OR DAMAGE NONMILT PROPERTY: $100 OR LESS
|7J5B2 |DESTROY OR DAMAGE NONMILT PROPERTY: MORE THAN $100
|7J6 |WRONGFUL DESTRUCTION OF PAY & ALLOWANCE DOCUMENTS
|7J7 |WRONGFUL DESTRUCTION OF COMMISSARY PROPERTY
|7J8 |WRONGFUL DAMAGING OF COMMISSARY PROPERTY
|7J9A1 |FAIL TO SECURE PROPERTY: $100 OR LESS
|7J9A2 |FAIL TO SECURE PROPERTY: MORE THAN $100
|7J9B1 |FAIL TO REPORT/TURN OVER PROPERTY: $100 OR LESS
|7J9B2 |FAIL TO REPORT/TURN OVER PROPERTY: MORE THAN $100
|7J9C1 |DEALING IN CAPTURED PROPERTY: $100 OR LESS
|7J9C2 |DEALING IN CAPTURED PROPERTY: MORE THAN $100
|7K |[RECEIVING STOLEN PROPERTY]
|7K |[RECEIVING STOLEN PROPERTY]
|7K1 |RECEIVING STOLEN PROP, OTHER ITEMS (NOT 7K2 - 7K8)
|7K2 |RECEIVING STOLEN DISPOSAL PROPERTY
|7K3 |RECEIVING STOLEN PROCUREMENT PROPERTY
|7K4 |RECEIVING STOLEN POL ITEMS
|7K5 |RECEIVING STOLEN POL RATION DOCUMENTS
|7K6 |RECEIVING STOLEN PAY & ALLOWANCES DOCUMENTS
|7K7 |RECEIVING STOLEN NONAPPROPRIATED FUND PROPERTY
|7K8 |RECEIVING STOLEN COMMISSARY PROPERTY OR ITEMS
|7K9 |RECEIVING STOLEN PROP USING A COMPUTER
7K0A STOLEN PROPERTY: RECEIVE/CONCEAL/BUY $100 OR LESS
7K0B STOLEN PROPERTY: RECEIVE/CONCEAL/BUY MORE THAN $100
|7K0C PROPERTY: SEIZURE, DESTRUCTION, REMOVAL
|7L |FAILURE TO PAY JUST DEBT
|7M |[REGISTRATION VIOLATIONS]
|7M1 |REGISTRATION VIOLATIONS, VEHICLE
|7M2 |REGISTRATION VIOLATIONS, FISH/GAME
|7M3 |REGISTRATION VIOLATIONS, OTHER
|7N |[ENVIRONMENTAL VIOLATIONS]
|7N1 |VIOL OF TOXIC SUBSTANCE ACT (15 USC 2605 SEC 6)
|7N2 |VIOL OF OSHA ASBESTOS ACT (29 USC 655/40 USC 333)
|7N3 |VIOL OF WATER CONTROL ACT (33 USC 1251-1387)
|7N4 |VIOL OF SAFE DRINKING WATER (42 USC 300 SEC J-6)
|7N5 |VIOL OF NAT ENVIR PROTECT ACT (42 USC 4321-4370A)

|7N5 |VIOL OF NAT ENVIR PROTECT ACT (42 USC 4321-4370A)
|7N6 |VIOL OF HAZ WASTE CONTROL ACT (42 USC 6901-6991L)
|7N7 |VIOL OF MEDICAL WASTE TRACKING (42 USC 6901)
|7N8 |VIOL OF CLEAN AIR ACT (42 USC 7401-7626/7418)
|7N9 |VIOL OF ENVIRONMENT RESP COMPENSATION/LIAB ACT
|7X |[OTHER CRIMES AGAINST PROPERTY]
|7X1 |SHOPLIFTING
|7X2 |CONSPIRACY
|7X3 |SOLICITATION TO COMMIT AN OFFENSE
|7X4 |ACCESSORY BEFORE THE FACT
|7X5 |ACCESSORY AFTER THE FACT
|7X6 |OBSTRUCTION OF JUSTICE

|8 |[FRAUD CRIMES]
|8A |[BRIBERY]
|8A1 |BRIBERY, OTHER THAN 8A2 - 8A5
|8A2 |BRIBERY, PROPERTY DISPOSAL
|8A3 |[BRIBERY, PROCUREMENT]
|8A3A |BRIBERY, PROCUREMENT - CONTRACT PROGRESS PAYMENTS
|8A3B |BRIBERY, PROCUR - REQUEST FOR PROP/INVIT FOR BID
|8A3C |BRIBERY, PROCUR - COST AND PRICE DATA
|8A3D |BRIBERY, PROCUR - CONTRACT NEGOTIATIONS
|8A3D |BRIBERY, PROCUR - CONTRACT NEGOTIATIONS
|8A3E |BRIBERY, PROCUR - DEFECTIVE MATERIALS
|8A3F |BRIBERY, PROCUR - RELEASE OF PROPRIETARY INFO
|8A4 |BRIBERY, PAY & ALLOWANCE MATTERS
|8A5 |BRIBERY, COMMISSARY MATTERS
|8A6 |BRIBERY, INVOLVING USE OF A COMPUTER
|8A7 |GRAFT
|8B |[CONFLICT OF INTEREST FRAUD]
|8B1 |CONFLICT OF INTEREST, OTHER
|8B2 |CONFLICT OF INTEREST, PROPERTY DISPOSAL
|8B3 |[CONFLICT OF INTEREST, PROCUREMENT]
|8B3A |CONFLICT OF INT, CONTRACT PROGRESS PAYMENTS
|8B3B |CONFLICT OF INT, REQ FOR PROPOSAL/INVIT FOR BID
|8B3C |CONFLICT OF INT, COST AND PRICE DATA
|8B3D |CONFLICT OF INT, CONTRACT NEGOTIATIONS
|8B3E |CONFLICT OF INT, DEFECTIVE MATERIALS
|8B3F |CONFLICT OF INT, RELEASE OF PROPRIETARY INFO
|8B4 |CONFLICT OF INTEREST, COMMISSARY
|8B5 |CONFLICT OF INTEREST, USE OF A COMPUTER
|8C |[DEPENDENCY ASSISTANCE FRAUD]
|8C1 |DEPENDENCY ASSISTANCE FRAUD
|8C2 |DEPENDENCY ASSISTANCE FRAUD USING A COMPUTER
|8C2 |DEPENDENCY ASSISTANCE FRAUD USING A COMPUTER

|8D |[PERSONNEL ACTION FRAUD]
1|8D1 |UNLAWFUL ENLISTMENT
|8D2 |UNLAWFUL SEPARATION
2 |8D3 |UNLAWFUL APPOINTMENT
|8D4 |FRAUD INVOLVING ASSIGNMENT/TRANSFER
|8D5 |FRAUD INVOLVING CIV PERSONNEL ACTIONS
|8D6 |[FRAUD INVOLVING COMMISSARY EMPLOYEES]
|8D6A |FRAUD INVOLVING COMMISSARY CIVIL SERVICE PERSONNEL
|8D6B |FRAUD INVOLVING COMMISSARY MILITARY PERSONNEL
|8D6C |FRAUD INVOLVING COMMISSARY CONTRACT PERSONNEL
|8D6D |FRAUD INVOLVING COMMISSARY CIVILIAN BAG BOYS/GIRLS
|8D7 |PERSONNEL FRAUD INVOLVING USE OF A COMPUTER
|8E |[NONAPPROPRIATED FUND FRAUD]
|8E1 |NAF FRAUD INVOLVING OFFICER'S OPEN MESS
|8E2 |NAF FRAUD INVOLVING NCO OPEN MESS
|8E3 |NAF FRAUD INVOLVING EM OPEN MESS
|8E4 |NAF FRAUD INVOLVING ROD & GUN CLUB
|8E5 |NAF FRAUD INVOLVING AAFES FACILITY
|8E6 |NAF FRAUD INVOLVING CENTRAL POST FUNDS
|8E7 |FRAUD INVOLVING OTHER NAF ACTIVITY
|8E7 |FRAUD INVOLVING OTHER NAF ACTIVITY
|8E8 |NAF FRAUD INVOLVING USE OF A COMPUTER
|8F |[PAY & ALLOWANCE FRAUD]
|8F1 |PAY & ALLOW FRAUD UNAUTHORIZED TRAVEL PAY FOR DEPS
|8F2 |PAY & ALLOW FRAUD COLLECTING DUPLICATE TRAVEL PAY
|8F3 |PAY & ALLOWANCE FRAUD INVOLVING TDY PAY
|8F4 |[PAY & ALLOW FRAUD PAY OTHER THAN TRAVEL OR TDY]
|8F4A |PAY & ALLOWANCE FRAUD INVOLVING BASE PAY (MIL/CIV)
|8F4B |PAY & ALLOW FRAUD QRTS, SUBSTENS & COST OF LIVING
|8F4C |PAY & ALLOW FRAUD ENLISTMENT/REENLISTMENT BONUS
|8F4D |PAY & ALLOW FRAUD HOUSEHOLD GOODS MOVEMENT
|8F5 |PAY & ALLOW FRAUD OTHER PAY & ALLOWANCE MATTERS
|8F6 |PAY & ALLOW FRAUD USE OF A COMPUTER
|8G |[PROCUREMENT, SALVAGE, PROPERTY DISPOSAL FRAUD]
|8G1 |PROCUREMENT FRAUD
|8G2 |[SALVAGE/PROPERTY DISPOSAL FRAUD]
|8G2A |SALVAGE/PROPERTY DISPOSAL FRAUD INV A PRIME CONT
|8G2B |SALVAGE/PROPERTY DISPOSAL FRAUD INV A SUB CONT
|8G3 |PROCUR, SALVAGE, PROP DISP FRAUD WITH A COMPUTER
|8H |[FRAUD INVOLVING POL ITEMS, DOCUMENTS, RATIONS]
|8H1 |FRAUD INVOLVING POL ITEMS (NOT RATION DOCUMENTS)
|8H1 |FRAUD INVOLVING POL ITEMS (NOT RATION DOCUMENTS)

|8H2 |FRAUD INVOLVING POL RATION DOCUMENTS
|8H3 |FRAUD INV POL ITEMS, DOCS, RATIONS WITH A COMPUTER
|8J |FRAUD PERTAINING TO MEDICAL TREATMENT
|8K |[ANTITRUST VIOLATIONS - CONTRACTORS]
|8K1 |ANTITRUST - CONTRACTORS, NOT PROC/COMM/AAFES/NAF
|8K2 |ANTITRUST VIOLATIONS - CONTRACTORS, COMMISSARY
|8K3 |ANTITRUST VIOLATIONS - CONTRACTORS, PROCUREMENT
|8K4 |ANTITRUST VIOLATIONS - CONTRACTORS, AAFES
|8K5 |ANTITRUST VIOLATIONS - CONTRACTORS, NAF
|8K6 |ANTITRUST VIOLATIONS - CONTRACTORS, PROP DISPOSAL
|8L |[WIRE FRAUD (18 USC 1343)]
|8L1 |[WIRE FRAUD NOT PROC/COMM/AAFESPROP DISP/NAF]
|8L1A |WIRE FRAUD REQUEST FOR CONTRACT PROGRESS PAYMENTS
|8L1B |WIRE FRAUD PROPOSAL/INVITATION FOR BID INFORMATION
|8L1C |WIRE FRAUD DISCLOSURE OF COST AND PRICE DATA
|8L1D |WIRE FRAUD INVOLVING CONTRACT NEGOTIATIONS
|8L1E |WIRE FRAUD INVOLVING USE OF DEFECTIVE MATERIALS
|8L1F |WIRE FRAUD INVOLVING RELEASE OF PROPRIETARY INFO
|8L2 |[WIRE FRAUD INVOLVING A COMMISSARY ACTIVITY]
|8L2A |WIRE FRAUD COMMISSARY ACTIVITY - PROGRESS PAYMENTS
|8L2A |WIRE FRAUD COMMISSARY ACTIVITY - PROGRESS PAYMENTS
|8L2B |WIRE FRAUD COMM ACTIVITY - PROPOSAL/INVITATION INF
|8L2C |WIRE FRAUD COMM ACTIVITY - DISCLOSURE OF COST DATA
|8L2D |WIRE FRAUD COMM ACTIVITY - CONTRACT NEGOTIATIONS
|8L2E |WIRE FRAUD COMM ACTIVITY - DEFECTIVE MATERIALS
|8L2F |WIRE FRAUD COMM ACT - RELEASE OF PROPRIETARY INFO
|8L3 |[WIRE FRAUD INVOLVING A PROCUREMENT ACTIVITY]
|8L3A |WIRE FRAUD: REQUEST FOR CONTRACT PROGRESS PAY
|8L3B |WIRE FRAUD: PROPOSAL/INVITATION FOR BID INFO
|8L3C |WIRE FRAUD: DISCLOSURE OF COST AND PRICE DATA
|8L3D |WIRE FRAUD: CONTRACT NEGOTIATIONS
|8L3E |WIRE FRAUD: USE OF DEFECTIVE MATERIALS
|8L3F |WIRE FRAUD: RELEASE OF PROPRIETARY INFORMATION
|8L4 |[WIRE FRAUD INVOLVING AN AAFES ACTIVITY]
|8L4A |WIRE FRAUD-AAFES-REQ FOR CONTRACT PROGRESS PAY
|8L4B |WIRE FRAUD-AAFES-PROPOSAL/INVIT FOR BID INFO
|8L4C |WIRE FRAUD-AAFES-DISCLOSURE OF COST AND PRICE DATA
|8L4D |WIRE FRAUD-AAFES-CONTRACT NEGOTIATIONS
|8L4E |WIRE FRAUD-AAFES-USE OF DEFECTIVE MATERIALS
|8L4F |WIRE FRAUD-AAFES-RELEASE OF PROPRIETARY INFO

|8L5 |[WIRE FRAUD INVOLVING A NAF INSTRUMENTALITY]
|8L5 |[WIRE FRAUD INVOLVING A NAF INSTRUMENTALITY]
|8L5A |WIRE FRAUD-NAF INSTR-REQ FOR CONTRACT PROGRESS PAY
|8L5B |WIRE FRAUD-NAF INSTR-PROPOSAL/INVIT FOR BID INFO
|8L5C |WIRE FRAUD-NAF INSTR-DISCLO OF COST AND PRICE DATA
|8L5D |WIRE FRAUD-NAF INSTR - CONTRACT NEGOTIATIONS
|8L5E |WIRE FRAUD-NAF INSTR - USE OF DEFECTIVE MATERIALS
|8L5F |WIRE FRAUD-NAF INSTR - RELEASE OF PROPRIETARY INFO
|8L6 |[WIRE FRAUD INVOLVING A PROPERTY DISPOSAL ACTIVITY
|8L6A |WIRE FRAUD-PDO- REQUEST FOR CONTRACT PROGRESS PAY
|8L6B |WIRE FRAUD-PDO ACT. PROPOSAL/INVIT FOR BID INFO
|8L6C |WIRE FRAUD-PDO ACT - DISCLO OF COST AND PRICE DATA
|8L6D |WIRE FRAUD INVOL A PDO ACTIVITY - CONTRACT NEGOTNS
|8L6E |WIRE FRAUD INVOL A PDO ACTIVITY - DEFECTIVE MATER.
|8L6F |WIRE FRAUD INVOL A PDO ACTIVITY - RELEASE OF INFO
|8L7 |MAIL FRAUD (18 USC 1341)
|8M |[PROCUREMENT FRAUD]
|8M1 |[PRODUCT SUBSTITUTION]
|8M1A |PRODUCT SUBSTITUTION INVOLVING CIVIL WORKS PROJS
|8M1B |PRODUCT SUBS INVOL MILITARY CONSTRUCTION PROJECTS
|8M1C |PRODUCT SUBSTITUTION INVOLVING MAINTENANCE
|8M1D |[PRODUCT SUBSTITUTION INVOL AVIATION COMPONENTS]
|8M1D |[PRODUCT SUBSTITUTION INVOL AVIATION COMPONENTS]
|8M1D1 |PRODUCT SUBS INVOLV TACTICAL AVIATION COMPONENTS
|8M1D2 |PRODUCT SUBS INVOL NON-TACT AVIATION COMPONENTS
|8M1E |[PRODUCT SUBSTITUTION INVOLVING VEHICLES]
|8M1E1 |PRODUCT SUBSTITUTION INVOLVING TACTICAL VEHICLES
|8M1E2 |PRODUCT SUBSTITUTION INVOLVING NON-TACTICAL VEHS
|8M1E3 |PRODUCT SUBSTITUTION INVOLVING ARMORED VEHICLES
|8M1F |PRODUCT SUBSTITUTION INVOLVING MISSILE SYSTEMS
|8M1G |PRODUCT SUBSTITUTION INVOLVING BIOLOGICAL AGENTS
|8M1H |PRODUCT SUBSTITUTION INVOLVING CHEMICAL AGENTS
|8M1J |PRODUCT SUBSTITUTION INVOLVING COMMO EQUIPMENT
|8M1K |PRODUCT SUBSTITUTION INVOLV FIRE CONTROL SYSTEMS
|8M1L |[PRODUCT SUBSTITUTION INVOLVING ARMAMENTS]
|8M1L1 |PRODUCT SUBSTITUTION INVOL LARGE BORE ARMAMENTS
|8M1L2 |PRODUCT SUBSTITUTION INVOL SMALL BORE ARMAMENTS
|8M1M |PRODUCT SUBSTITUTION INVOLVING COMPUTER SYSTEMS
|8M1N |[PRODUCT SUBSTITUTION INVOLVING MUNITIONS]
|8M1N1 |PRODUCT SUBSTITUTION INVOLVING CONVENTIONAL EXPL
|8M1N2 |PRODUCT SUBSTITUTION INVOL SMALL ARMS MUNITIONS
|8M1N3 |PRODUCT SUBSTITUTION INVOLVING NUCLEAR MUNITIONS

|8M1N4 |PRODUCT SUBSTITUTION INVOLVING BIO MUNITIONS
|8M1N4 |PRODUCT SUBSTITUTION INVOLVING BIO MUNITIONS
|8M1N5 |PRODUCT SUBSTITUTION INVOLVING CHEMICAL MUNITIONS
|8M2 |PROCUR FRAUD INVOLVING DEFECTIVE MATERIALS
|8M3 |PROCUR FRAUD INV DEFECTIVE COST AND PRICE DATA
|8M4 |PROCUREMENT FRAUD INVOLVING COST MISCHARGING
|8M5 |PROCUREMENT FRAUD INVOLVING LABOR MISCHARGING
|8M6 |PROCUR FRAUD SUPPL CODE: OFFS BY PRIME CONTRACTOR
|8M7 |PROCUR FRAUD SUPPL CODE: OFFS BY SUBCONTRACTOR
|8M8 |PROCUR FRAUD SUPPL CODE: CONTRACTOR PLANT REP OFC
|8P |[COMPUTER FRAUDS - FEDERAL INTEREST COMPUTER]
|8P1 |COMPUTER FRAUDS - OBTAINING CLASSIFIED INFORMATION
|8P2 |COMPUTER FRAUDS - OBTAINING FINANCIAL/CREDIT INFO
|8P3 |COMPUTER FRAUDS - UNAUTH ACCESS AFFECTING OPNS.
|8P4 |COMPUTER FRAUDS - ACCESS WITH INTENT TO DEFRAUD
|8P5 |COMPUTER FRAUDS - ALTER/DAMAGE/DEST INFO, >$1000
|8P6 |COMPUTER FRAUDS - ALTER/DAMAGE/DEST MEDICAL INFO)
|8P7 |COMPUTER FRAUDS - TRAFFICKING PASSWDS/ACCESS CODES
|8P8 |COMPUTER FRAUDS - SUPPLEMENTAL CODE (ATTEMPTS)
|8Q |[RESTRICTIONS ON POST-GOVERNMENT EMPLOYMENT]
|8Q1 |RECEIVING UNAUTHORIZED COMPENSATION (18 USC 203)
|8Q2 |EMPLOYEE AS AGENT OF PVT INDIV/ENTITY (18 USC 205)
|8Q2 |EMPLOYEE AS AGENT OF PVT INDIV/ENTITY (18 USC 205)
|8Q3 |POST-EMPLOYMENT RESTRICTIONS (18 USC 207)
|8Q4 |UNAUTH RECEIPT OF DUAL COMPENSATION (18 USC 209)
|8Q5 |NEGOTIATING FOR EMPLOYMENT (10 USC 2397)
|8Q6 |ACTS FOR PERSONAL FINANCIAL INTEREST (18 USC 208)
|8Q7 |VIOL OF EMPLOYMENT RESTRICTIONS FOR RET MIL OFF
|8Q8 |VIOLATION OF HARBORD AMENDMENT (37 USC 801)
|8Q9 |VIOL OF FED PROCUREMENT POLICY ACT (41 USC 423)
|8R |[WORKER’S COMPENSATION FRAUD]
|8R1 |FALSE STATEMENT (18 UC 1920)
|8R2 |RECEIVING COMPENSATION AFTER MARRIAGE (18 USC 1921
|8R3 |FALSE OR WITHHELD REPORT (18 USC 1922)
|8R4 |FRAUDULENT RECEIPT OF PAYMENT (18 USC 1923)
|8S1 |BAD CHECK: DEFRAUD $100 OR LESS
|8S2 |BAD CHECK: DEFRAUD MORE THAN $100
|8S3 |BAD CHECK: DECEIVE
|8S4 |CHECK:WORTHLESS MAKE/UTTER (BAD FAITH/GROSS

	INDEFFE
|8R1	|FRAUD: MAKE FALSE CLAIM
|8R2	|FRAUD: PRESENT FALSE CLAIM
|8R3	|FRAUD: FALSE DOCUMENT WITH CLAIM
|8R4	|FRAUD: FALSE OTH IN CONNECTION WITH CLAIM
|8S1	|FRAUD: FORGERY OF SIGNATURE
|8S2	|FRAUD: USE FORGED SIGNATURE
|8T1	|DELIVER LESSER AMT THAN ON RECEIPT: $100 OR LESS
|8T2	|DELIVER LESSER AMT THAN ON RECEIPT: MORE THAN $100
|8U1	MAKE/DELIVER RCPT W/OUT FULL KNOWL: $100 OR LESS
|8U2	|MAKE/DELIVER RCPT W/OUT FULL KNOWL: MORE THAN $100
|8V1	|FALSE PRETENSE: $100 OR LESS
|8V2	|FALSE PRETENSE: $MORE THAN $100
|8W	|BURN WITH INTENT TO DEFRAUD
|8X	|[OTHER FRAUD OFFENSES]
|8X1	|INVOLVING USE OF A COMPUTER (SUPPLEMENTAL CODE)
|8X2	|CONSPIRACY
|8X3	|SOLICITATION TO COMMIT AN OFFENSE
|8X4	|ACCESSORY BEFORE THE FACT
|8X5	|ACCESSORY AFTER THE FACT
|8X6	|OBSTRUCTION OF JUSTICE
	(8Y Offense Codes are pending the utilization of ACI2)
|8Y	|FRAUDULENT USE OF GOVERNMENT CREDIT CARDS
|8Y1	|FRAUDULENT USE OF THE U.S. GOVT PURCHASE CARD
|8Y2	|FRAUDULENT USE OF THE U.S. GOVT TRAVEL CARD
|9	|[SPECIAL INVESTIGATIVE ACTIVITIES]
|9A	|[CRIME SURVEY]
|9A1	|CRIME ANALYSIS (CRIME TRENDS AT AN INSTALLATION)
|9A1A	|CRIME ANALYSIS - CRIMES AGAINST PERSONS
|9A1B	|CRIME ANALYSIS - CRIMES AGAINST PROPERTY
|9A1C	|CRIME ANALYSIS - GENERAL (COMB OF CATEGORIES)
|9A1C	|CRIME ANALYSIS - GENERAL (COMB OF CATEGORIES)
|9A1D	|CRIME ANALYSIS - OTHER
|9A1E	|DRUG ASSESSMENTS
|9A2	|CPS-LOGISTICAL (DPDO, AMMUNITION PLANTS, ETC)
|9A3	|CPS-INSTALLATION SUPPORT ACTIVITIES (CLUBS, ETC)
|9A4	|PERSONNEL SECURITY ASSESSMENTS
|9B	|INDUSTRIAL SURVEY
|9C	|[CIVIL LITIGATION]
|9C1	|FALSE CLAIMS ACT (31 USC 3729)
|9C2	|PROGRAM FRAUD CIVIL REMEDIES ACT (31 USC 3801)
|9D	|[MILITARY WORKING DOGS]
|9D1	|[NARCOTICS/CONTRABAND DETECTOR DOG]
|9D1A	|DRUG DETECTION DOGS - MARIJUANA
|9D1B	|DRUG DETECTION DOGS - HASHISH

|9D2 |EXPLOSIVES DETECTOR DOG
|9D3 |PATROL DOG
|9E |PHYSICAL SECURITY SURVEY
|9F |PROTECTIVE SERVICES
|9G |[SCIENTIFIC EXAMINATIONS]
|9G1 |POLYGRAPH EXAMINATION
|9G2 |[CRIME LABORATORY ANALYSIS]
|9G2 |[CRIME LABORATORY ANALYSIS]
|9G2A |CHEMISTRY
|9G2B |FINGERPRINTS
|9G2C |FIREARMS
|9G2D |DOCUMENTS
|9G2E |PHOTOGRAPHY
|9G2F |OTHER
|9G3 |INVESTIGATIVE HYPNOSIS
|9H |CRIMINAL INFORMATION
|9J |WAR CRIMES
|9K |[VOLUNTARY DISCLOSURE INVESTIGATIONS]
|9K1 |VOLUNTARY DISCLOSURE INVEST I/PRIME CONTRACTOR
|9K2 |VOLUNTARY DISCLOSURE INVEST I/SUBCONTRACTOR
|9L |[QUI TAM INVESTIGATION]
|9L1 |Q.T. INVESTIGATION INVOLVING A PRIME CONTRACTOR
|9L2 |QUI TAM INVESTIGATION INVOLVING A SUBCONTRACTOR
|9M |[TOP 100 DEFENSE CONTRACTOR INVESTIGATIONS]
|9M1 |PROCUR. CONTRACTOR AWARDED TO A TOP 100 CONTRACTOR
|9M2 |CONTRACT AWARDED TO A SUBSIDARY OF A TOP 100
|9R |REVERSE DRUG OPERATION
|9T |[UNIT & INDIVIDUAL TRAINING]
|9T |[UNIT & INDIVIDUAL TRAINING]
|9T1 |UNIT TRAINING ACTIVITY
|9T2 |INDIVIDUAL TRAINING
|9T3 |BASIC TRAINING
|9W |ELECTRONIC SURVEILLANCE

Appendix B
Major Command Assignment Codes (MCAC)

B-1. Definition.

A major command assignment code is a two position code used to identify major commands or major subordinate commands as listed in appendix B, AR 71-14 (The Department of the Army, The Army Authorization Documents System) and Joint Pub 1-03.3 (Joint Reporting Structure Status of Resources and Training System).

B-2. Use.

The command codes will be entered into the ACIRS database to identify the major command or major subordinate command for each subject and victim.

B-3. Major command and subordinate command assignment codes:

COMMAND/MAJOR SUBORDINATE COMMAND CODE

1R
First US Army

5R
Fifth US Army

AE
Army Acquisition Executive Support Agency

AR
Army Reserve

AS
US Army Intelligence and Security Command (INSCOM)

AU
US Army Audit Agency

CB
US Army Criminal Investigation Command (CIDC)

CE
US Army Corps of Engineers (COE)

CS
Army Staff

CT
Army Central Command

CZ
US Army Information Systems Command (ISC)

DF
DOD Agencies

DJ
US Special Opns Cmd/Subordinate Commands

DM
Directed Military Overstrength

E1
US Army, Europe & Seventh Army

E2
21st Theater Area Command & 5th TAACO

E3
Southern European Task Force

E5
V Corps

E6
94th Air Defense Artillery Brigade

E8
30th Medical Brigade

EA
Reserved for Contingency Use

EB
First Personnel Command

EC
Preposition Materiel Unit Sets (POMCUSI), USAMMAE

ED
26th Support Group, Military Community Heidelberg

EF
US Army Civilian Support Group

EQ
Reserved for Wartime Contingency Use

ER
US Army Reserve, Europe

ES
Reserved for Wartime Contingency Use

ET
Reserved for Wartime Contingency Use

EU
Reserved for Wartime Contingency Use

EV
Reserved for Wartime Contingency Use

EX
Reserved for Wartime Contingency Use

FC
US Army Forces Command (FORSCOM)

FZ
FORSCOM GFRE Support to Reserve Components

GB
National Guard Bureau

HR
Compo 1 Managed by USARC

J1
US Army Element Supreme HQ Allied Powers Europe

JA
Joint Activities (Less SHAPE)

KR
US Army Reserve, EUSA

MA
US Military Academy (USMA)

MC
US Army Medical Command (MEDCOM)

MP
US Total Army Personnel Command (PERSCOM)

MT
Military Traffic Management Command

MW
US Army Military District of Washington (MDW)

NG
National Guard Units (Not On Active Duty)

P1
US Army Pacific (USARPAC)

P8
Eight US Army (EUSA)

PR
US Army Reserve, Pacific

SA
Office, Secretary of the Army

SB
FOAs of the Secretariat

SC
US Army Space and Strategic Defense Command

SE
ARSTAF FOAS (Resourced by OA-22)

SF
ARSTAF FOAS (Not Resourced by OA-22)

SJ
Secretary Army, Joint and Support Activities

SP
USA Special Opns Cmd/Major Subordinate Cmds

SR
US Army Reserve, Special Operations Command

SS
Staff Support Agencies of the Secretariat

SU
US Army South (USARSO)

TA
US Army Recruiting Command (USAREC)

TC
US Army Training & Doctrine Command (TRADOC)

TM
US Army Military Entrance Processing Command

X1
US Army Materiel Command (AMC)

X2
Headquarters USAMC

X3
Headquarters Staff Support Activities

X4
Training Activities

X5
AMC All Other

X6
Missile Command

X7
Tank Automotive & Armaments Command

X8
Communications & Electronics Command

X9
Simulation Training & Instrumentation Command

XA
Chemical & Biological Defense Command

XB
Aviation and Troop Command

XC
Soldier Systems Command

XD
Research Laboratory

XK
Materiel Acquisition Activities

XL
Materiel Acquisition Project Managers

XM
Test & Evaluation Command

XP
Security Assistance Command

XQ
Industrial Operations Command

XT
Test, Measurement, & Diagnostic Equipment Activity

B-4. Other Codes

XX
Materiel Readiness Activities

XY
Foreign Nationals Employed by DOD

XZ

All Other Foreign Nationals Not Connected to DOD

ZZ
US Citizens Not DOD Affiliated

B-5. Special instructions

a. U.S. civilian employees of the U.S. Army will be coded according to the command or activity to which their organization is assigned.

b. Retired Service members, regardless of Service affiliation, will be coded according to the major command or activity where the incident occurred.

c. U.S. civilian DoD employees (employed by other than U.S. Army) will be coded DF (Defense agencies).

d. Military and civilian Army-Air Force Exchange Service (AAFES) employees will be coded JA (Joint activities).

e. U.S. Army Non-appropriated Fund (NAF) civilian employees will be coded according to the major command/activity responsible for operation of the installation on which employed.

f. Foreign military personnel assigned/attached to a U.S. Army element will be coded with the MCAC of that U.S. Army element.

g. U.S. military family members will be coded the MCAC of the sponsor's major command.

h. Other U.S. military personnel (non-Army) will be coded DF (Defense Agencies).

Note: Some of these organizations were deactivated, however; the organization names and codes are listed for reference to past reports and records.

Appendix C
Hypnosis Policy

C-1. General.

Hypnosis can be used as an investigative tool to assist willing witnesses and/or victims in recalling important additional information regarding particular crimes, contributing to solving the crime, or allowing more timely apprehension of the subject(s).

C-2. Use of hypnosis

a. Cases which are considered best suited for hypnosis should either: (1) already contain evidence with which to confirm hypnotically developed information, or (2) involve witnesses or victims whose hypnotic recall might reasonably be expected to yield evidence which is corroborable. To ensure that helpful results of hypnosis will be attained, a review of the investigation must reveal that a witness or victim was likely exposed to investigatively important factors. Further, this exposure must have occurred under conditions in which the individual's perception of additional information appears likely. If a suspect has been identified in the investigation, hypnosis is probably contraindicated because its primary purpose has already been served. Additionally, only serious cases warrant the use of hypnosis, and even then, the hypnosis technique is employed only after all other logical, traditional investigative techniques have been exhausted. The only possible exception may be in cases of intense priority, such as those involving the potential loss of life.

b. Hypnosis is confined to use only with key witnesses or victims of crimes. No individual who has the potential of becoming a suspect or subject in an investigation is to be hypnotized for any reason. A statement of consent will be obtained from each witness or victim being hypnotized.

c. All leads developed through hypnosis should be verified with supporting physical or testimonial evidence. Investigative conclusions will not be based solely on information obtained through hypnosis.

d. Hypnosis will not be used to determine a witness' or victim's truthfulness pertaining to any aspect of an investigation.

C-3. Legal coordination

a. USACIDC field elements anticipating the use of hypnosis must obtain the concurrence of the supported installation staff judge advocate. In those

investigations being conducted jointly with another law enforcement agency, concurrence is also required from the appropriate United States attorney or civilian prosecutor.

b. Legal issues which cannot be resolved at the field element level will be forwarded to the respective USACIDC major subordinate command judge advocate.

C-4. Requests for hypnosis interviews

a. Requests for approval of hypnosis interviews will be forwarded to the respective USACIDC major subordinate command headquarters. Requests will contain, as a minimum, the following information:

(1) The USACIDC ROI number.

(2) A synopsis of the incident under investigation.

(3) The identity and relationship of the individual to be hypnotized to the investigation.

(4) The identity of the hypnotist who will conduct the hypnosis interview.

(5) A statement of the results desired from the hypnosis interview.

b. Hypnosis interviews should only be considered after traditional interview techniques fail. Contact the appropriate command forensic science coordinator for assistance and recommended alternatives.

C-5. Approvals

All hypnosis interviews conducted pursuant to criminal investigations in which the USACIDC is the sole or primary investigative agency will require prior approval of the respective USACIDC major subordinate commander, following a legal review of the request by the major subordinate command judge advocate. In the absence of the major subordinate commander, the deputy major subordinate commander is authorized to approve the request. This authority may not be further delegated.

C-6. Qualifications of hypnotists.

Hypnosis will only be induced by a licensed psychiatrist, psychologist, or physician who has received specialized hypnosis training, possesses clinical

experience in the use of hypnosis techniques, and is a member o r is eligible for membership in either the American Society of Clinical Hypnosis, the Society of Clinical and Experimental Hypnosis, or the International Society of Hypnosis.

C-7. Locating the hypnotist

a. The USACIDC field element requesting the use of hypnosis may, if deemed appropriate, identify a local licensed psychiatrist, psychologist, or physician possessing the qualifications listed in paragraph C-6 above, to induce the hypnosis interview. If the local field elements is unable to locate a qualified hypnotist, that field element will request assistance from the respective major subordinate command forensic science coordinator in locating a qualified hypnotist to participate in t he hypnosis interview. In the event the major subordinate command forensic science coordinator is unable to identify a qualified hypnotist, that forensic science coordinator will contact the HQUSACIDC forensic science coordinator for assistance. The HQUSACIDC forensic science coordinator will then contact the Office of the Surgeon General, Department of the Army or Walter Reed Army Medical Center for assistance.

b. Qualified professionals identified to participate in hypnosis interviews for the USACIDC must conduct the hypnosis interviews in accordance with this appendix.

C-8. Payment of fees

a. When a civilian hypnotist is used to induce hypnosis pursuant to USACIDC investigations, payment of fees will normally be made in accordance with AR 37-1, appendix G (Desk Reference Guide for Commercial Accounts).

b. In those instances in which one or more of the conditions described in AR 195-4, paragraph 1-6b, can be applied and documented, payment may be made from Contingency Limitation .0015 Funds in accordance with AR 195-4.

C-9. Pre-hypnosis interview

a. USACIDC field elements will obtain a detailed sworn statement from the witness or victim (hereafter referred to as interviewee) prior to the hypnosis interview. A sworn statement is necessary to ensure that all details recalled by the interviewee without benefit of hypnosis are recorded. This interview, to include obtaining of the sworn statement, should be video taped, with prior written consent of the interviewee.

b. It is paramount that the interviewee not be allowed to form an impression of the investigation or gain inside knowledge of the status of the investigation. Before the induction of hypnosis, it is important that any new elements not be added to the interviewee's description of the facts and circumstances of the incident.

C-10. Hypnosis interview (general)

a. A trained forensic hypnosis coordinator (if available) or the case agent will be responsible for arranging the interview. The hypnotist will be provided with a copy of this appendix for familiarization with the USACIDC hypnosis policy. A special agent (or hypnosis coordinator) who has detailed knowledge of the case will brief the hypnotist prior to the interview to ensure that no leading or suggestive questions are asked. The hypnotist should not be briefed on specific details of the incident. The hypnotist should only be briefed as to the nature, approximate date, time and location of the incident, and any general type of information desired by the hypnotist to further assist in the interview. This briefing will be videotaped and retained as evidence in accordance with paragraph 5-10d of this regulation and AR 195-5 (Evidence Procedures).

b. The hypnosis interview will also be videotaped and will be retained as evidence. During the video recording of the interview, the interviewee, special agent, and hypnotist will be in camera view. The special agent will provide case administrative information, identity of all present, and time/date/location of the interview at the beginning of the tape recording.

c. The hypnotist will have complete control of inducing, maintaining, and terminating the hypnotic trance placed upon the interviewee. Any decision to terminate the trance in consideration of the interviewee's welfare will be made only by the hypnotist. A USACIDC special agent will not actively participate in this phase of the interview.

d. Once the trance is induced, the special agent will question the interviewee with assistance from the hypnotist, as needed. Normally, the hypnotist will not ask detailed questions unless trance enhancing techniques are required. It is desirable to have the interviewee provide an uninterrupted description of the incident while under hypnosis. The interviewee may then be asked to respond to specific questions about the incident with either verbal or ideomotor responses as determined by t he hypnotist. Special agents should use a list of questions previously discussed with the interviewee. Additional questions will be asked to develop the information provided by the interviewee.

e. When obtaining descriptions, identi-kit composites, or presenting lineups, the interviewee should be brought out of the hypnotized state after refreshing his/her memory, and an attempt made to obtain the desired information using normal

interview techniques. If this is not successful, the information may be sought while the interviewee is in the hypnotic trance.

f. In the event the interviewee makes a self-incriminating statement warranting investigation while in the hypnotic trance, the interview will be terminated immediately. The interviewee will be brought to full consciousness and advised of the statement made while under hypnosis and that it cannot be used against him/her. The interviewee will then be advised of his/her rights and interviewed as a suspect using normal interview techniques.

C-11. Hypnotic interview procedure and content

a. Preparation of setting:

(1) Select a place where quiet can be assured with no interruptions. Have a good, comfortable chair for the interviewee.

(2) TV equipment set up and fully functioning (cameras, recorder, monitor, clock, microphones).

(3) Sufficient supply of video tape.

(4) Consent form(s) available.

(5) Clipboard, paper, pens, etc.

(6) Photo lineup, identi-kit and/or artist materials.

(7) Prepare video operator to signal about five minutes before tape needs to be changed.

b. The interview (EVERYTHING IS ON TAPE). The special agent:

(1) Opens the interview with a statement that provides the location, date, time, and identification of all persons present.

(2) Requests and receives permission from the interviewee to record the entire proceeding on video tape. Should the interviewee not provide permission to be video taped, ensure the proceeding is witnessed by an independent person.

(3) States the purpose of the interview.

The hypnotist:

(4) Explains hypnosis (which may include):

(a) Asking the interviewee if he/she has been previously hypnotized.

(b) Asking what the interviewee knows/has heard about hypnosis.

(c) Defining hypnosis.

(d) Explaining misconceptions about hypnosis.

(e) Describing trance characteristics and experimental qualities.

(5) Explains procedures to be used (which may include):

(a) Trance induction.

(b) Deepening time distortion.

(c) Mentions potential "risks" (e.g., re-experience of emotions connected with the event.)

(d) Inquiry techniques (e.g., T.V. technique, etc.).

(e) Post-hypnotic suggestion.

(f) Obtains informed consent.

(g) Returns attention to the special agent.

The special agent:

(h) Obtains the interviewee's signature on the consent form. Before the interviewee signs the form, the special agent asks "Are you in hypnosis now?" (A negative reply is necessary.)

(i) Asks the interviewee to describe the incident under investigation. This is a detailed recounting, allowing the interviewee to review the events as he or she desires.

The hypnotist:

(j) Conducts suggestibility test (optional).

(k) Conducts induction (may use practice inductions).

(l) Tests trance depth by observing/enacting hypnotic phenomena.

The special agent and hypnotist together:

(m) Conducts inquiry (use present tense)

(1) Let the interviewee describe the event spontaneously, or with minimal encouragement. After the entire event is related the first time, follow with a detailed description, assisted with T.V. techniques, etc.

(2) If descriptions are obtained in trance, have the interviewee report them again following the termination of trance. (The hypnotist may use post-hypnotic suggestions to assist in providing descriptions out of trance).

(n) If the interviewee makes a self- incriminating statement warranting investigation, the hypnotist must terminate the trance, have the interviewee acknowledge (verbally) that he/she is out of trance.

(o) Terminates trance (last thing to be done before termination of video taping is to ask the interviewee "How do you feel?"). Be sure tapes include interviewee's response.

(p) Asks the interviewee to report what he/she said in trance; develop details (this discussion is to evidence enhanced memory). Obtain a sworn statement if necessary.

(q) Ends interview. Say aloud the time indicated on the clock, and announce that the interview is concluded.

c. Breaks

(1) Breaks will be needed to change tape, use rest room facilities, or possibly allow for meals. Trance should terminate before breaks, and (on tape) a precautionary statement not to discuss the case.

(2) The hypnotist will terminate and re-initiate the trance(s) as needed.

C-12. Checklist for special agents.

Safeguards to be used when hypnosis is to be used to restore the interviewee's memory:

a. Medical history information.

b. Interview of hypnotist by both parties (defense and prosecution).

c. Interview should be conducted by an independent mental health professional experienced in the use of hypnosis.

d. The hypnotist should not be regularly employed by either parties (defense or prosecution).

e. Any information concerning the case which is revealed to the hypnotist by either party must be recorded in some manner, preferably videotape.

f. A detailed statement from the interviewee prior to the hypnosis interview.

g. The interview will be conducted in a neutral location.

h. A post session statement documenting pertinent information provided by the interviewee during the hypnosis session.

C-13. Documenting hypnosis interviews

a. The fact that an individual was interviewed under hypnosis, the identity of the hypnotist, and a synopsis of the results of the interview will be recorded in the narrative portion of the ROI.

b. Audio and video tapes of hypnosis interviews will be listed in the "not attached" exhibits section of the final ROI. Transcripts of the audio tapes may be attached as separate exhibits to the final ROI.

C-14. Special distribution requirements.

A copy of all video and audio recordings of hypnosis interviews will be forwarded to HQUSACIDC, ATTN; CIOP-CO-PE for assessment and research. A complete copy of the final ROI should also accompany the recordings.

Appendix D
Criminal Investigation Standards

D-1. Purpose.

This appendix establishes standards for the USACIDC criminal investigation program and explains related USACIDC Inspector General evaluation procedures.

D-2. Applicability.

This appendix applies to Headquarters, United States Army Criminal Investigation Command, all subordinate units, and any other CID elements of the Department of the Army when conducting criminal investigation operations.

D-3. Investigative mission

a. The success of the USACIDC effort cannot be measured solely by solved versus unsolved cases. The solve rate does serve as a useful indicator of investigative success. However, a solved case may not have been thoroughly investigated nor all pertinent factors developed. Conversely, a thorough and professional investigation may result in an unsolved case. Therefore, successful investigative effort must be evaluated against the broader standard of whether all available factors have been developed and reported with sufficient clarity and timeliness to permit appropriate action. This determination is subjective in part, but certain aspects can be evaluated objectively in comparison with announced standards.

b. The USACIDC must accomplish its investigative mission in a compressed time frame to effectively support the Army. The transient nature of society means that timeliness in conducting an investigation may affect its successful completion. Timeliness in reporting the investigation is also important because of judicial requirements for speedy resolution of allegations.

c. If the USACIDC is to be successful in accomplishing its mission, special agents must:

(1) Verify that an offense within USACIDC investigative jurisdiction has or has not been committed.

(2) Identify the offenders.

(3) Locate the offenders (except those re-ported as deserters which are monitored by CRC).

(4) Exonerate persons incorrectly accused or suspected of criminal conduct.

(5) Gather, record, and provide to the supported commander facts which substantiate the culpability of, or exonerate, a suspect.

(6) Support the judicial system and remedy officials with admissible evidence.

D-4. Inspections

a. Inspections are heavily weighted in the investigative operations area; however, all functional areas (supervision, personnel and administration, organization, training, logistics, and resource management), will be inspected and considered in determining the overall evaluation of a unit.

b. Evaluation of the investigative operations will be determined in part by:

(1) The percentage of investigative actions investigated in a timely and thorough manner.

(2) The percentage of investigative actions reported in a timely manner.

(3) The effectiveness of support programs in accomplishing the investigative process.

c. All factors are considered in evaluating a unit's performance, including the condition that existed in the unit during the inspected period, as well as those on the date of the inspection. Supervisors at all levels are expected to recognize problems and take appropriate action to correct the situation, within the resources available, and notify the next higher headquarters when the solution is beyond the unit commander's control.

d. The perceptions and comments of the supported commanders and their staffs, concerning the quality of the investigative support, will be considered in the determination of the overall evaluation of the unit.

D-5. Investigative standards

a. The USACIDC investigative standards are grouped into three general categories:

(1) Investigations - paragraph D-6.

(2) Organization and management - paragraph D-7.

(3) Investigative Support programs - paragraph D-8.

b. These standards have not been derived arbitrarily, but represent a collective determination by this headquarters and field units as to what constitutes minimum acceptable standards of performance in the conduct of criminal investigation activities. The standards have been established in furtherance of the USACIDC goal to increase professionalism. Whenever possible, all USACIDC personnel and units should strive to exceed the standards and maintain a higher level of performance.

c. Investigative standards will be modified by the HQUSACIDC as necessary to reflect what is practically attainable by USACIDC units.

D-6. Investigations.

The listed standards, while not all inclusive, will be considered when evaluating any investigative action for timeliness, thoroughness, and timely reporting. Whenever these standards are not met for a valid reason, an explanation will be noted on the Agent's Activity Summary (AAS) in the case folder.

a. Timely investigative effort. When, at a minimum, 85 percent of the cases inspected document timely investigative effort, the unit inspected will be considered fully successful in regards to the timeliness of investigative activity. The following are timeliness standards:

(1) Crime scenes are responded to promptly.

Note: For the purposes of MPFU, the term, crime scenes, includes, but is not limited to, a contractor facility, contracting officer files, administrative contracting officer files, finance and/or accounting records. Crime scenes may not be accessible or controlled by USACIDC agents without a search warrant or subpoena.

(2) Initial interviews of victims and eyewitnesses are conducted within 24 hours of their being identified, if reasonably available.

(3) Interviews of significant witnesses (i.e., complainants, sources, CQs, roommates, etc) or other persons (including those agreed upon with the SJA/AUSA) who may have direct knowledge of the crime are conducted within five working days, if reasonably available.

(4) Meaningful follow-up investigation is undertaken in a timely manner which precludes the loss of perishable evidence, either physical or testimonial.

(5) Meaningful investigative activity is continuous and accomplished without unjustified time gaps, normally ten working days, or within a reasonable time frame. Time gaps in excess of ten working days will not be considered reasonable unless authorized and substantiated by the special agent-in-charge.

(6) Physical evidence is entered into the evidence depository by the end of the next working day.

(7) Evidence evaluated for laboratory examination is submitted to the USACIL within five working days of determining the need for such examination and required supporting evidence (standards, exemplars, etc.), has been collected.

(8) Polygraph examination requests are submitted within five working days after the need for the examination is identified.

(9) Requests for assistance (RFA) are dispatched within five working days of the recognition of the need.

(10) Requests for assistance are followed-up within 15 working days of receipt unless unusual circumstances exist.

(11) Requests for assistance from other agencies are accomplished and replies dispatched within 15 working days of receipt, unless circumstances exist which make a reply unavailable within the specified time.

b. Thorough investigative effort. When, at a minimum, 90 percent of the cases inspected document a thorough investigative effort, the unit inspected will be considered fully successful in regards to the thoroughness of investigative effort. The following are thoroughness standards:

(1) Inquiries and investigations are responded to and properly initiated.

(2) A professional preliminary inquiry is conducted with a timely, thorough, and well documented crime scene search.

(3) Crime scene evidence, to include trace evidence, is identified, collected, and evaluated.

(4) Other evidence is identified, collected and evaluated throughout the investigation.

(5) Crime scene photography and/or sketches are accomplished as necessary to support the investigative effort.

(6) Polygraph examinations are requested and conducted when appropriate.

(7) Information in the ROI is supported by the case file and inconsistencies are identified and resolved where possible.

(8) Credible information and evidence are available to support the cited offense and the listing of the subject.

(9) Adequate efforts are made to develop leads through the use of criminal intelligence files, registered, and other sources, and are recorded in the AAS.

(10) All reasonable leads are pursued except where early termination is authorized.

(11) Alibis and other defenses are identified, investigatively developed, and timely pursued.

(12) Legal coordination is conducted with the appropriate SJA/AUSA and recorded in the ROI narrative.

Note: Legal coordination is essential in some incidents and may be considered a deficiency if not done promptly.

(13) Requests for assistance are conducted in a thorough manner (the requested action is accomplished to the extent possible, based on available and developed information) and properly documented.

c. Timely reporting of investigative effort. When, at a minimum, 90 percent of the cases inspected document a timely reporting of investigative effort, the unit inspected will be considered fully successful in regards to timely reporting of investigative effort. The following are timely reporting standards:

(1) Significant developments during the investigation are promptly reported to interested commanders, prosecuting attorneys, other authorized recipients (Procurement Fraud Advisor, AUSA, etc.), and the notification entered on the AAS.

(2) Investigative activity is fully documented as soon as possible.

(3) Investigative reports (initials, status, interims, finals or supplementals) are provided to the action commander, prosecuting attorney and other authorized recipients (such as HQUSACIDC) as required by this regulation.

(4) Initial and status reports documenting investigative developments are dispatched within the time limits established by this regulation.

(5) Known subject final, supplemental, and monitored ROIs are dispatched within 15 working days of the last meaningful investigative activity. Known subject cases that have had final disciplinary action completed, and all other unknown subject final, supplemental ROIs, and unfounded finals are dispatched within 30 working days. Supervisory (SAC or Operations Officer) review may be considered meaningful investigative activity if appropriate to the circumstances (i.e., supervisory direction that additional work be conducted or that investigative activity be terminated and a final prepared).

Note: For the purpose of the MPFU, error free input into ACIRS (DIMIS information) is effected within 72 hours of the final signature execution of the remedy.

d. Reasonable Application of Standards by the USACIDC Inspector General.

(1) During the conduct of compliance inspections IG Technical Inspectors will not annotate timeliness, thorough-ness, and timely reporting shortfalls as deficiencies if the unit:

(a) Identified and documented the deficiency and root cause of the shortfalls in sufficient time and corrected the shortfalls in such a manner that it had no irrevocable impact on the overall progress and effectiveness of the investigation, or reporting requirements; and

(b) Addressed the shortfall through appropriate action such as unit training; individual counseling; change to unit policy; and

(c) Properly documented the action taken to correct the root cause of the shortfall.

(2) In determining if the deficiency will be annotated, the effect the shortfall had on the case as a whole will be considered. The final decision that the error did not detract from the investigative effort will be made by the inspector.

(3) The intent of this policy is to provide investigative supervisors at all levels with positive reinforcement for conducting and documenting timely case review and providing guidance to their offices. This policy will not excuse patterns of substandard performance or systematic weaknesses and training shortfalls

D-7 Organization and management standards

a. General. These standards are designed to enhance the effectiveness of the unit's organization and management in accomplishing the investigative mission.

Deficiencies in these areas may cause an evaluation of weakness if the unit's effectiveness is impaired.

b. Management and functions

(1) Adequate unit goals and objectives are established and consistent with those of HQUSACIDC.

(2) An SOP is in effect which provides clear, concise instructions on the functioning of the unit. SOPs will not repeat or consolidate policies and procedures prescribed in other publications and documents that are available to the unit (paragraph 7-6b, FM 101-5).

(3) Unit personnel are assigned duties and responsibilities consistent with their TDA/MTOE positions.

Note: For the purpose of MPFU, replace TDA/MTOE positions with position descriptions.

(4) Investigative teams are functioning, where appropriate, with team chiefs directly responsible for team members and their investigations.

Note: For the purpose of MPFU, team chiefs are replaced with SAC s and team members with unit members.

(5) Subordinate resident agencies and branch offices are adequately supervised and supported by the commander and staff.

Note: For the purpose of MPFU, resident agencies are replaced with fraud field offices and branch offices replaced with fraud resident agencies.

(6) The commander is maintaining adequate performance data to assist in evaluating unit mission accomplishment.

(7) All aspects of criminal investigation activity are effectively integrated in the unit's investigative operations.

c. Supervision

(1) Supervisors at all levels are concerned with the professional and personal welfare of military and/or civilian subordinates.

(2) The appropriate supervisor is discussing the case investigative plan with the special agents as necessary.

(3) Supervisors are managing the progress and meaningfully influencing the course of the investigation.

(4) Supervisors are reviewing investigative activity and correcting deficiencies or misdirection in a timely manner.

(5) Supervisors are effectively integrating criminal intelligence, hypnosis, .0015 funds, registered sources, polygraph, evidence, crime records, and crime laboratory support sub-programs into the investigative process.

(6) Supervisors are managing in a manner that allows sufficient time to observe and supervise field activity.

(7) Team chiefs (SAC s for MPFU) are effectively used as first line supervisors of the special agents.

(8) Supervisors are entering investigative and administrative guidance in the AAS of case folders they review. This will not include performance related commands due to disclosure requirements under criminal/civil actions.

(9) Supervisors are ensuring that copies of completed DA Forms 4833 are forwarded to the USACRC in a timely manner.

(10) Supervisors are ensuring that the unit is preparing and forwarding FD Forms 249 (FBI Criminal History Fingerprint Cards) and FBI/DOJ Forms R-84 (Final Disposition Reports) in accordance with policies established by this regulation (see Paragraph 7-31 and Appendix 0).

(11) Supervisors are ensuring that status reports documenting administrative developments (such as corrected social security numbers or full names) are dispatched as soon as possible in accordance with this regulation

D-8. Investigative support programs standards

a. General. Successful mission accomplishment will depend to a large extent on how effectively the units and the special agents integrate a number of support programs into the overall investigation program. These support programs involve crime prevention surveys, criminal intelligence and source management, counter terrorism/force protection, drug suppression, polygraph examinations, .0015 funds, crime records, evidence, crime laboratory support, liaison, training, and investigative equipment. The Inspector General's interest in these support programs centers around the extent to which all investigative personnel have implemented, managed, and integrated the support programs into the investigation program, and how well they make use of the support programs.

Note: For the purpose of MPFU, terrorism, drug suppression, and counteraction, support programs are not applicable.

b. The Crime Prevention Survey (CPS) Program. The CPS program is evaluated primarily on the adequacy of the unit's program in meeting USACIDC goals and objectives in crime prevention and the effect the surveys have on the investigative programs. The following areas are considered important:

(1) The number of unit generated CPSs performed is consistent with the unit's capabilities.

(2) The surveys are developed from the analysis of information from TAFs, ROIs, CIRs, AAA, Inspector General, and other source reports on activities.

(3) The criminal intelligence manager is involved in the process of identifying recommended targets/surveys.

(4) The TAFs are scheduled to preclude conflicts with other management reviews and inspections.

(5) The TAFs/CPSs of large activities are limited in scope, where possible.

(6) The training and experience of the special agents is considered when assigning surveys.

(7) The TAFs/CPSs are preplanned with achievable goals.

(8) The supported command is briefed on the scope of the surveys.

(9) Special agents are conducting surveys in a timely and thorough manner.

(10) The surveys are providing the supported commander with an understandable, realistic evaluation and practical recommendations for improvement.

(11) Commander's reports of action taken on CPSs are suspense for receipt within 90 days with effective timely procedures established for following up on those not received within 90 days.

(12) The supported commanders and the staff (DIO, IG and PM) are satisfied with the quantity and quality of the crime prevention survey support.

Note: For the purpose of MPFU, replace the staff (DIO, IG and PM) with program manager.

c. Criminal Intelligence Program. The Criminal Intelligence Program is evaluated primarily on the degree to which it contributes to identifying, solving and preventing crime and how registered sources are utilized to identify, solve and prevent crime. The following areas are considered important:

(1) Special agents are knowledgeable about the criminal intelligence program, understand what information is available, and how to retrieve it.

(2) Criminal intelligence data is readily available to special agents at all times.

(3) Special agents are utilizing criminal intelligence in their investigations.

(4) Investigations and, where possible, TAFs and CPSs are initiated from criminal intelligence when appropriate.

(5) Routine systemic USACIDC procedures are being used to obtain criminal intelligence.

(6) Criminal intelligence collection objectives are identified and meaningful effort is directed toward collecting the information.

(7) A continuous, systematic analysis of criminal intelligence is being accomplished to identify areas requiring investigative action and crime trends.

(8) The unit’s management of sources identifies areas where sources are needed and special agents are developing source information accordingly.

(9) Special agents are registering sources, as appropriate.

(10) Special agents are maintaining contact with registered sources, providing them with guidance on functions, and effectively targeting their activities.

(11) Registered source contacts are being fully documented in case files and cross-referenced on CID Forms 20.

(12) The source control officer is managing sources effectively in support of investigations.

(13) Sources are being properly identified in case files and having their reliability established.

(14) Special agents are providing appropriate protection to registered sources before, during, and after utilization.

(15) Analysis and dissemination of collected, time-sensitive information concerning the criminal threat against Army interests is taking place.

(16) Liaison with Federal, State and local agencies (to include host country agencies) to exchange criminal intelligence is being conducted.

(17) Domestic criminal intelligence collection efforts are being conducted and domestic criminal threat information is being disseminated (to include remote installations).

(18) A close working relationship has been established with the supporting 902nd MI Group element.

(19) The unit has a copy of the supported commander's priority intelligence requirements (PIR) and has directed collection efforts in support of those requirements.

d. Drug Suppression Program. The Drug Suppression Program is evaluated primarily by analyzing the nature and extent of the drug abuse problem of the supported command, reviewing the drug suppression activities of the unit to counter these problems, and assessing the effectiveness of the program. The following areas are considered important:

(1) The unit has a drug suppression plan with objectives and it is realistically being implemented.

(2) The unit has a drug coordinator or team chief who is knowledgeable of duties and responsibilities.

(3) A continuous analysis is being made to assess the nature and extent of drug abuse.

(4) The unit is initiating an appropriate number of its own drug investigations and not excessively dependent upon outside sources.

(5) The unit is effectively using confidential funds, sources, criminal intelligence, and special investigative equipment in its drug suppression program.

(6) The unit has a CID/MPI drug suppression effort where possible.

f. Polygraph examinations. Polygraph examination activities are evaluated primarily on the degree of utilization in solving investigations or exonerating suspects. The following areas are considered important:

(1) Special agents are identifying the need for a polygraph examination in a timely manner.

(2) Special agents are discussing the desirability of a polygraph examination with the supporting polygraph examiner within five working days of identifying the need.

(3) Polygraph examinations are being requested and processed expeditiously by the unit.

(4) Polygraph examinations are being conducted as expeditiously as possible after identification of the need.

g. Contingency limitation .0015 funds. The use of .0015 funds is evaluated primarily on how effectively the funds are used and administered in accomplishing the investigative mission. The following areas are considered important:

(1) Special agents thoroughly understand the uses and limitations of .0015 funds.

(2) The .0015 funds are readily available to special agents and used appropriately.

(3) Special agents and supervisors are exhibiting reasonable care in safeguarding and recovering .0015 funds without unduly restricting fund utilization.

(4) Recovered .0015 funds are being returned to use expeditiously.

(5) Approving officials are conducting periodic comparisons of .0015 fund vouchers with the investigative files.

(6) Approving authorities are conducting periodic unannounced cash fund counts of the contingency funds maintained by the fund custodian.

h. Crime records. The use of crime records is evaluated primarily based on the effective utilization of records information during investigative activities. The following areas are considered important:

(1) Crime records checks are initiated promptly for all suspects and complainants, victims, and witnesses whose statements appear improbable or whose motives are unclear.

(2) Crime records checks are made promptly on each new registered source.

(3) The results of records checks are entered in the AAS/source files as appropriate.

i. Evidence procedure and crime laboratory support. Evidence procedures and crime laboratory support are evaluated primarily on the efficient and timely handling, examination, and disposition of the evidence. The following areas are considered important:

(1) The evidence custodian organizes the evidence room efficiently and manages its operation effectively.

(2) The evidence custodian logs all evidence immediately upon receipt and ensures that the evidence is properly marked and tagged.

(3) The evidence custodian initiates requests for disposition approvals within five working days of when the submission is possible.

(4) The disposition of evidence is accomplished within 10 working days of the receipt of disposition approval.

(5) The need for laboratory examination of evidence is identified in a timely manner.

(6) Evidence is submitted to the USACIL within five working days of the identification of the need for the examination.

(7) Laboratory requests are submitted which identify the investigative need and provide background information with sufficient clarity to enable laboratory examiners to provide responsive support.

(8) Results of laboratory analysis are provided to the interested special agent immediately upon receipt.

(9) An inquiry is made to the supporting USACIL and noted in the AAS when results are not received within three weeks of submission for expedite requests and six weeks for routine requests.

(10) The evidence room is inspected and inventoried as required by AR 195-5.

j. Liaison activities. Liaison activities are evaluated primarily on the degree of personal relationship, cooperation, mutual respect, and confidence between the unit and other organizations which lead to effective mission accomplishment.

k. Training programs. The training program is evaluated primarily on how well the unit is accomplishing the training and meeting requirements in AR 350-1 and the Command Training Implementation Guidance (CTIG). In addition, the following areas are considered important:

(1) Apprentice agents are assigned investigative tasks appropriate to their training and experience.

Note: For the purpose of MPFU, this program is applicable for special agents in the grades of GS 09 and GS 11.

(2) The commander structures the training program to correct investigative deficiencies attributed to inadequate training.

Note: For the purpose of MPFU, the SAC will structure the appropriate training.

(3) The unit training program contributes to developing and increasing special agent's investigative expertise in new investigative concepts, procedures, and equipment.

(4) Apprentice agent evaluation is conducted in accordance with CID Pam 195-5.

Note: For purpose of MPFU, apprentice agent is replaced with agent trainee,

(5) Support personnel are actively involved in the training program.

l. Investigative equipment activities. Investigative equipment activities are evaluated primarily on how knowledgeable key individuals having responsibility for these activities are aware of new techniques and equipment, and how well they integrate techniques and equipment into the investigative program. The following areas are considered important:

(1) The status, condition and availability of investigative equipment.

(2) Agent knowledge of publications, films, and other training sources relating to the use of investigative equipment and techniques.

(3) The unit procedures for familiarizing special agents with new or modified investigative equipment and effectiveness of the techniques.

m. Economic Crime Program. The Economic Crime Program is evaluated primarily by analyzing the nature and extent of the economic crime threat of the supported command, reviewing the economic crime- related activities of the unit to counter the threat, and assessing the effectiveness of the program. The following areas are considered important:

(1) Criminal intelligence is being maintained and a continuous analysis is being made to assess the nature and extent of the economic crime threat.

(2) The ECTA identifies all potential economic crime targets, the targets are prioritized, and plans of attack are formulated on the high priority targets.

(3) The unit is effectively integrating and using confidential funds, sources, criminal intelligence, and special investigative equipment in its economic crime program.

(4) The TAFs are generally being scheduled and conducted on appropriate economic crime targets that have been identified as high priorities in the ECTA. Furthermore, CPSs are being initiated from TAFs, economic crime investigative act ions, or in support of requests for surveys.

(5) Sources are being recruited and targeted in activities that have been identified as high priorities in the ECTA.

(6) The .0015 funds are being utilized to maximum advantage in attacking high priority targets.

(7) The high priority targets identified in the ECTA are being appropriately attacked through the use of one or more of the available investigative programs.

(8) The unit is initiating an appropriate number of its own economic crime investigations and is not excessively dependent upon outside referrals.

n. Terrorism Counteraction Program. The Terrorism Counteraction Program is evaluated primarily on the readiness of the unit to provide support to the local community in the areas of hostage negotiation, crisis reaction and vulnerability assessments. The following areas are considered important:

(1) That high risk personnel (HRP) in the area of responsibility have been identified and that vulnerability assessments have been offered and/or conducted.

(2) That the unit has trained hostage negotiators available to provide support to the local community when requested or required by crisis reaction plans.

(3) That the unit is participating in the preparation of installation/area crisis reaction plans and maintain and exercise those plans.

(4) The unit is an active member of the local AT/force protection (FP) Committee.

(5) Appropriate liaison is taking place with elements operating in support of AT/FP Programs.

(6) Appropriate criminal threat and vulnerability assessments are being conducted for Army installations, systems, operations and other interests.

(7) Appropriate AT/FP training is being accomplished.

(8) The unit maintains a major incident response plan.

(9) The unit is represented in the installation EOC.

(10) The CID Battalion has a formally trained and certified AT officer.

(11) The unit is executing the Army AT standards outlined in AR 525-13.

o. Safety Program. This program is evaluated primarily on the training of personnel concerning safety measures exercised during investigative/law enforcement operations, and other areas which might jeopardize the safety or well being of assigned personnel and personnel that might be encountered during CID operations. This includes safety/protective equipment readiness and availability for assigned personnel. The following areas are considered important:

(1) Protective vests are serviceable, fit properly and are available for investigative/law enforcement operations.

(2) Radio communications equipment is operational and used when necessary.

(3) Weapons are in good working condition, and properly carried during CID operations/duty.

(4) Weapon training is conducted in accordance with chapter 17 of this regulation.

(5) Duty vehicles are equipped with safety and emergency equipment and the equipment is in good condition.

(6) All special agents are currently validated as having successfully completed the cardiopulmonary resuscitation and emergency cardiac care examination.

Appendix E
Liaison Program

E-1. Purpose.

This appendix sets forth the objectives, principles, and policies of the USACIDC with regard to liaison responsibilities.

E-2. Explanation of terms

a. Liaison. Intercommunication established between elements of the USACIDC and supported DA/DoD elements, and between the USACIDC and other law enforcement agencies to ensure mutual understanding, unity of action, and prompt effective support by the USACIDC.

b. Liaison responsibilities. A USACIDC program encompassing both official liaison officers who function as an operational extension of the commander and normal operational or staff contact and coordination with DA/DoD commands/agencies and with other law enforcement elements.

c. Liaison officer (LNO). An officer identified by the USACIDC to represent the USACIDC to a specific Army command or federal investigative agency.

E-3. Objective.

This program is designed to improve relationships and foster cooperation with other law enforcement agencies, with DA/DoD agencies/elements, and with other major Army commands. Effective liaison is vital to USACIDC mission accomplishment.

E-4. Policies

a. Liaison or coordination between HQUSACIDC staff elements and the comparable staff elements of supported DA/DoD command/agency is a normal procedure and is not intended to be restricted or inhibited by the provisions of this regulation, or by the designation of a liaison officer to the supported DA/DoD element.

b. The USACIDC-MACOM LNOs are an operational extension of the Commanding General, USACIDC, and as such, represent the USACIDC to the supported MACOM commander. The USACIDC-MACOM LNOs are authorized direct contact with USACIDC elements Army-wide and are granted tasking

authority to the degree required to perform liaison responsibilities. All USACIDC elements have the responsibility to provide applicable data, (via telephone, electrical message, and/or letter) to designated USACIDC-MACOM LNOs for proper mission accomplishment.

c. The USACIDC federal liaison officer (FLO) represents the USACIDC to federal criminal investigative agencies located in the Washington, DC, area.

d. All official liaison functions will be conducted under the supervision of the Deputy Commander, USACIDC, except for those of the FLO.

e. Protective services. Provisions of this regulation are not intended to inhibit or restrain necessary liaison or activities of the Protective Services Unit (PSU). Threat information pertaining to principals will be exchanged routinely between the PSU and those organizations, commands, or activities with a need to know.

E-5. Responsibilities

a. General. All elements of the USACIDC will establish and maintain local liaison programs. Such programs will include liaison and coordination with supported Army organizations, activities, and agencies within the geographic area of responsibility of the USACIDC elements, and with appropriate DoD, law enforcement, and other government agencies located within the USACIDC element's geographical area of responsibility.

b. The USACIDC major subordinate commanders will maintain liaison with MACOMs located in their respective AORs, contacting them at least quarterly. The USACIDC major subordinate Commanders may delegate day-to-day liaison functions to subordinate USACIDC elements.

c. MACOM liaison officers (LNOs). The USACIDC-MACOM LNOs have the responsibility to:

(1) Maintain continuity in the exchange of essential information pertaining to the USACIDC and the supported MACOM.

(2) Promote cooperation and coordination of effort through personal contact with the supported command.

(3) Remain informed of USACIDC activities concerning the supported MACOM and make this information available to the commander and staff of the supported MACOM.

(4) Make continuing reports on matters within the scope of the mission of the USACIDC. Maintain appropriate records, and advise the commander of the

supported MACOM of information about his command provided to HQUSACIDC by the LNO.

(5) Remain informed of MACOM activities concerning impact upon the USACIDC and advise the Commander, USACIDC, of the information as expeditiously as possible.

d. Federal liaison officer (FLO). The FLO is responsible to the Commander, USACIDC:

(1) Establish and maintain continuity in the exchange of essential information pertaining to the USACIDC and other federal and foreign criminal investigative agencies.

(2) Promote cooperation and coordination of effort through personal contact with the federal and foreign criminal investigative agencies in the Washington, DC area.

(3) Remain informed of USACIDC activities that impact on federal and foreign criminal investigative agencies and make this information available to the appropriate federal or foreign agency.

(4) Remain informed of other federal and foreign criminal investigative agencies' activities and their impact upon the USACIDC and advise the Commander, USACIDC, of this information as expeditiously as possible.

(5) Represent the command to International Association of Chiefs of Police (IACP), Law Enforcement Exploring and other professional organizations.

(6) Maintain appropriate records.

E-6. Liaison assignments

a. The FLO, assigned to HQUSACIDC, will accomplish liaison with the following activities:

(1) Central Intelligence Agency (CIA)

(2) Federal Aviation Administration (FAA)

(3) General Services Administration (GSA) to include the Federal Protective Service (FPS)

(4) HQ, Air Force Office of Special Investigations (AFOSI)

(5) HQ, Defense Criminal Investigative Service (DCIS)

(6) HQ, Defense Investigative Service (DIS)

(7) HQ, Naval Criminal Investigative Service (NCIS)

(8) International Criminal Police Organization (INTER-POL)

(9) Royal Canadian Mounted Police (RCMP)

(10) Securities and Exchange Commission (SEC)

(11) Office of Personnel Management (OPM)

(12) U.S. Department of Agriculture (USDA)

(13) U.S. Department of Justice (DOJ) to include:

(a) Drug Enforcement Administration (DEA)

(b) Federal Bureau of Investigation (FBI)

(c) Immigration & Naturalization Service (INS)

(d) U.S. Marshal Service

(14) U.S. Department of State (USDS)

(15) U.S. Department of Treasury, to include:

(a) Internal Revenue Service (IRS)

(b) U.S. Customs Service (USCS)

(c) U.S. Secret Service (USSS)

(d) Bureau of Alcohol, Tobacco and Firearms (BATF)

(16) U.S. Park Police (USPP)

(17) U.S. Postal Service (USPS)

(18) Veterans Administration (VA)

b. Liaison with the following commands and activities will be accomplished by the USACIDC element indicated:

(1) I Corps: Commander, 6th MP Group

(2) III Corps: Commander, 11th MP Bn

(3) XVIII Corps: Commander, 10th MP Bn

(4) Army Materiel Command: Director, MPFU

(5) Forces Command: Commander, 3rd MP Group

(6) 3rd Army: Commander, 3rd MP Group

(7) 1st Army: Commander, 3rd MP Group

(8) 5th Army: SAC, Fort Sam Houston RA

(9) U.S. Army Special Operations Command: Commander, 10th MP BN (CID)(Abn), Fort Bragg, NC

(10) U.S. Army Training and Doctrine Command (TRADOC): SAC, 12th MP Det (CID), Ft Eustis, VA

(11) U.S. Army Troop Support Agency (TSA): SAC, Fort Lee RA

(12) Combined Arms Support Command: SAC, Fort Lee RA

(13) Army Intelligence and Security Command: DCSOPS

(14) Corps of Engineers: Director, MPFU

(15) Army Medical Command: SAC, Fort Sam Houston RA

(16) Military Traffic Management Command: Director, MPFU

(17) U.S. Army Europe and 7th Army: Commander, 202nd MP Group

(18) Army Pacific: Commander, Hawaii Field Office

(19) 8th Army: Commander, 19th MP Bn

(20) Army South: SAC, Puerto Rico RA

(21) Army National Guard: Commander, Washington District

(22) Army Reserve Component: Commander, 3rd MP Group

(23) Army Recruiting Command: SAC, Fort Knox RA

(24) U.S. Military Academy: SAC, West Point RA

(25) U.S. Army Japan: Commander, 19th MP BN

(26) U.S. Army Strategic Defense Command: Commander, Washington District

(27) SHAPE: Commander, 202nd MP Group

(28) U.S. Special Operations Command: Commander, Fort Benning District

(29) U.S. Joint Forces Command: SAC, 12th MP Det

(30) U.S. Pacific Command: Commander, Hawaii Field Office

(31) U.S. Transportation: Director, MPFU

(32) U.S. Central Command: Commander, Fort Benning District

(33) U.S. European Command: Commander, 202nd MP Group

(34) U.S. Space Command: DCSOPS

(35) U.S. Southern Command: Commander, Fort Benning District

(36) U.S. Strategic Command: Commander, Fort Riley District

(37) Defense Commissary Agency: SAC, Fort Lee RA

(38) Southern European Task Force: SAC, Vicenza RA

(39) Army and Air Force Exchange Service: Commander, 11th MP BN

(40) Defense Logistics Agency: DCSOPS

(41) U.S. Army Military Police School: DCSOPS

(42) Joint Task Force-Command: DCSOPS

(43) ACERT: Commander, CCIU

(44) LIWA: Commander, CCIU

(45) CONUS RCERT: Commander, CCIU

(46) Defense Finance and Accounting Office (DFAS): Resident Agent in Charge (RAC), Indianapolis Fraud Resident Agency, MPFU, USACIDC, 8899 East 56th Street Building 1, Column 101-C, Indianapolis, IN 46249-4801, (ifra.cid@us.army.mil).

d. Commanders and operations officers will maintain continuing liaison with commanders and other criminal investigative agencies in their area of responsibility.

Appendix F
Cooperation with Civilian Law Enforcement Officials (CLEO) Report

F-1 Purpose. This Appendix establishes policy and clarifies procedures for completing the quarterly CLEO Report. Further, it also establishes levels of approval authority for providing various types of support to civilian law enforcement officials.

F-2 Requirements. DoD Directive 5525.5 (DoD Cooperation with Civilian Law Enforcement Officials) requires that the Department of the Army cooperate with civilian law enforcement officials to the greatest extent possible, provided the request does not affect national security or military preparedness. In CONUS, USACIDC major subordinate commands (MSC) will complete a quarterly report IAW the format in figure F-1. USACIDC MSCs are required to collect CLEO statistics from subordinate field elements and electronically transmit one consolidated report to HQUSACIDC, ATTN: CIOP-COP, NLT 5 working days after the end of the quarter.

F-3 Reportable Categories. The eight reportable categories on the CLEO report are facilities, information, equipment, personnel, ground-based mission support, explosive ordnance disposal support, training, and aviation mission support. Within each of the categories, the reportable items, approval authority, and non-reportable items are as follows:

a. Facilities:

1. Reportable Items: This pertains to loans of buildings, classrooms, office space, and other such structures for the exclusive use of civilian law enforcement authorities for non-military interest actions.

2. In most instances, the use of facilities may require approval or notification of the installation chain of command. Approval authority within USACIDC is as follows:

(a) Use less than 24 hrs, SAC approval required.

(b) Use over 24 hrs, BN/FO commander approval required.

(c) Use over 48 hrs, MSC Commander approval required.

3. Non-Reportable Items: Reporting requirements do not apply to the use of facilities in conjunction with collateral, referred or joint investigations or actions having a military interest.

b. Information:

1. Reportable Items: This pertains to the providing of information, technical advice or training in performing investigative actions in support of civilian law enforcement when there is no military interest or involvement. To preclude potential violations of the Posse Comitatus Act, all such requests for involvement of USACIDC personnel to provide information, training or advice in active civilian law enforcement operations off-post with no military interest or involvement should be reviewed by the MSC SJA.

2. Approval authority

(a) On scene advice and assistance, regardless of duration, BN/FO commander approval required.

(b) Personnel interviews, regardless of duration, BN/FO commander approval required.

(c) Other requests, not included in the non-reportable criteria below, require BN/FO commander approval.

3. Non-Reportable Items: Investigative efforts in support of joint, collateral, or referred investigations or actions will not be reported. The reporting requirements do not apply to requests for information requiring less than two hours to complete, such as local file checks, alpha roster checks, worldwide locator checks, requests for local records or photographs, and local name checks from USACIDC/MP files. USACIDC field units are prohibited from conducting checks of CRC files for civilian authorities concerning non-military related matters or for employment screening. Requests of this nature must be submitted by the requesting agency directly to the U.S. Army Crime Records Center, 6010 6th Street, Fort Belvoir, VA 22060.

c. Equipment:

1. Reportable Items: This pertains to the loan of Army property to civilian law enforcement for activities that have no military interest or involvement.

2. Approval authority

(a) Arms and Ammunition: USACIDC units do not have authority to loan any weapons or ammunition to civilian law enforcement. All such requests must be forwarded through HQUSACIDC, ATTN: CIOP-ZA to HQDA (DALO-SMS) for approval.

(b) Technical Listening Equipment (TLE) or other sensitive equipment: For less than 90 days, MSC commander approval is required. For periods over 90 days, HQUSACIDC approval is required.

(c) Other USACIDC equipment: For less that 90 days, BN/FO commander approval is required. For periods over 90 days, MSC Commander approval is required.

3. Non-Reportable Items: Investigative equipment used in support of joint, collateral, or referred investigations or actions will not be reported.

d. Personnel:

1. Reportable Items: This pertains to the temporary or extended assignment or loan of USACIDC personnel to civilian law enforcement agencies in support of non-military actions. To preclude potential violations of the Posse Comitatus Act, all such requests requiring the loan or assignment of USACIDC personnel in civilian law enforcement operations off-post with no military nexus should be reviewed by the MSC SJA.

2. Approval authority:

(a) Less than 24 hours, SAC approval required.

(b) Greater than 24 hours, but less than 48 hours, BN/FO commander approval required.

(c) Greater than 48 hours, but less than 30 days, MSC commander approval required.

(d) Greater than 30 days, HQUSACIDC approval required.

3. Non-Reportable Items: Investigative personnel involvement in support of joint, collateral, or referred investigations or actions will not be reported.

e. Ground-Based Mission Support: This is not applicable to CID as it pertains to radar/sensor support, National Guard demonstration support, support to the Immigration and Naturalization Service, detector dog service and advisor support.

f. Training: This is not applicable to CID as it pertains to dog handling, security, flight training, ranger school training, and small unit tactics.

g. Explosive Ordnance Disposal (EOD) Support: This is not applicable to CID as it pertains to support provided by U.S. Army EOD organizations.

h. Aviation Mission Support: This is not applicable to CID, as it pertains to aircraft support provided by U.S. Army aviation organizations.

F-4. Reporting Format. The following format (figure F-1) will be used by CONUS based USACIDC MSCs (including USACIL and USACRC) to report the unit's consolidated information.

Appendix G
DoD Hotline Program

This DoD program provides any concerned individual the opportunity to report suspected fraud, waste, and/or abuse of DoD. The report may either be telephonic or written. Once a report is rendered, action must be taken to investigate that report. A single Army Hotline Office (AHO) has been established to manage, monitor, and report to DoD the actions and findings of audits, inspections, and investigations of all Hotline allegations pertaining to the Army. After analyzing the substance of each allegation, the AHO refers the allegation to the appropriate Army agency for action. Those allegations determined to be criminal in nature are referred to the Office of the Deputy Chief of Staff for Operations, for further dissemination to the USACIDC major subordinate command responsible for the inquiry/investigation. The Office of the Deputy Chief of Staff for Operations screens all referred Hotline reports to ensure the allegation is within the purview of the USACIDC, UP AR 195-2, and returns those that are not to the AHO.

a. On receipt of a DoD Hotline allegation, the USACIDC field element will:

(1) Conduct a preliminary inquiry to be completed within 90 days.

(2) If the preliminary inquiry does not disclose credible information that a crime has occurred, then submit a DoD Hotline Completion Report within 90 days from the date of the receipt of the allegation. All documents supporting the unfounded inquiry will be attached. (See figure G-1).

(3) If the preliminary inquiry cannot substantiate or refute the allegation within 90 days, submit a DoD Hotline Progress Report. (See figure G-2). Subsequent DoD Hotline Progress reports will be submitted every 90 days thereafter until:

(a) The allegation is determined to be unfounded and a DoD Hotline Completion Report is submitted, or;

(b) The allegation is substantiated and an ROI is initiated (see (4) below).

(4) If the allegations are substantiated and an ROI is initiated, the field element must include CDR USACIDC WASH DC//CIOP-CO// in the "TO" address line of the initial and all status reports. Each report will contain both the Hotline and the HQUSACIDC control number. Sixty days after the dispatch of the initial ROI, a DoD Hotline Progress Report will be submitted. Subsequent DoD Hotline Progress Reports will be submitted every 60 days thereafter until submission of the final ROI.

(5) A DoD Hotline Completion Report will only be submitted along with the final ROI (with exhibits) when command/judicial action has been received. If command/judicial action has not been received when the final ROI is approved by the CID commander, or special agent-in-charge, then a DoD Hotline Progress Report will be submitted along with a copy of the final ROI with exhibits. In either case, a DoD Hotline Completion Report will be submitted within 15 days of the receipt of the commander's report of action.

(6) Telephonic communications may be used to provide time sensitive, hotline interim report information; however, telephonic communications will not suffice for the basis of reports to the AHO.

(7) DoD Hotline Progress Reports sent by electrical or electronic message will conform to the format in figure G-2, and will be addressed as in (4) above. All DoD Hotline Progress/Completion Reports and associated documents submitted by mail will be addressed to Commander, USACIDC, ATTN: CIOP-CO (Hotline). In any case, Hotline Progress Reports will contain detailed information concerning the progress of the investigation, and not simply state, "Investigation Continues."

b. If investigative jurisdiction of a DoD Hotline allegation is referred to another investigative agency, i.e., FBI, ATF, IRS, MPI, Provost Marshal, etc., the responsible USACIDC field element will:

(1) Submit a DoD Hotline Progress Report detailing the circumstances surrounding the referral and maintain liaison with the agency to which the investigation was referred.

(2) Submit a DoD Hotline Progress Report to HQUSACIDC every 90 days thereafter until completion of the investigation and the report of commander's action/judicial action is received. At that time, the USACIDC field element will submit a DoD Hotline Completion Report with a copy of the investigative agency's report attached as an enclosure.

c. If a USACIDC field element receives a request for an investigation regarding a DoD Hotline complaint from another agency, i.e., Corps of Engineers Security, Defense Logistics Agency Security, local Inspector General, etc., the following provisions apply:

(1) Inform the referring agency that the Hotline complaint must be returned, through channels, to the AHO. The AHO will formally task the USACIDC to conduct the inquiry, in accordance with AR 195-2.

(2) If the referring agency challenges established procedures, then a telephonic report should be submitted through command channels to CDR, USACIDC, ATTN: CIOP-CO.

(3) Sufficient information may be obtained from the referring agency to conduct a preliminary investigation to substantiate or refute the allegation(s). However, it will be made clear to the referring agency that this action does not constitute acceptance of the referral by or on behalf of the USACIDC.

(4) DoD Hotline Progress or Completion Reports are not required from USACIDC field elements until tasked to provide them by HQUSACIDC. All hotline reports will be completed in accordance with this regulation and forwarded only to HQUSACIDC. The HQUSACIDC will review the report(s) and make any distribution outside of USACIDC channels.

Appendix G
DoD Hotline Program

This DoD program provides any concerned individual the opportunity to report suspected fraud, waste, and/or abuse of DoD. The report may either be telephonic or written. Once a report is rendered, action must be taken to investigate that report. A single Army Hotline Office (AHO) has been established to manage, monitor, and report to DoD the actions and findings of audits, inspections, and investigations of all Hotline allegations pertaining to the Army. After analyzing the substance of each allegation, the AHO refers the allegation to the appropriate Army agency for action. Those allegations determined to be criminal in nature are referred to the Office of the Deputy Chief of Staff for Operations, for further dissemination to the USACIDC major subordinate command responsible for the inquiry/investigation. The Office of the Deputy Chief of Staff for Operations screens all referred Hotline reports to ensure the allegation is within the purview of the USACIDC, UP AR 195-2, and returns those that are not to the AHO.

a. On receipt of a DoD Hotline allegation, the USACIDC field element will:

(1) Conduct a preliminary inquiry to be completed within 90 days.

(2) If the preliminary inquiry does not disclose credible information that a crime has occurred, then submit a DoD Hotline Completion Report within 90 days from the date of the receipt of the allegation. All documents supporting the unfounded inquiry will be attached. (See figure G-1).

(3) If the preliminary inquiry cannot substantiate or refute the allegation within 90 days, submit a DoD Hotline Progress Report. (See figure G-2). Subsequent DoD Hotline Progress reports will be submitted every 90 days thereafter until:

(a) The allegation is determined to be unfounded and a DoD Hotline Completion Report is submitted, or;

(b) The allegation is substantiated and an ROI is initiated (see (4) below).

(4) If the allegations are substantiated and an ROI is initiated, the field element must include CDR USACIDC WASH DC//CIOP-CO// in the "TO" address line of the initial and all status reports. Each report will contain both the Hotline and the HQUSACIDC control number. Sixty days after the dispatch of the initial ROI, a DoD Hotline Progress Report will be submitted. Subsequent DoD Hotline Progress Reports will be submitted every 60 days thereafter until submission of the final ROI.

(5) A DoD Hotline Completion Report will only be submitted along with the final ROI (with exhibits) when command/judicial action has been received. If command/judicial action has not been received when the final ROI is approved by the CID commander, or special agent-in-charge, then a DoD Hotline Progress Report will be submitted along with a copy of the final ROI with exhibits. In either case, a DoD Hotline Completion Report will be submitted within 15 days of the receipt of the commander's report of action.

(6) Telephonic communications may be used to provide time sensitive, hotline interim report information; however, telephonic communications will not suffice for the basis of reports to the AHO.

(7) DoD Hotline Progress Reports sent by electrical or electronic message will conform to the format in figure G-2, and will be addressed as in (4) above. All DoD Hotline Progress/Completion Reports and associated documents submitted by mail will be addressed to Commander, USACIDC, ATTN: CIOP-CO (Hotline). In any case, Hotline Progress Reports will contain detailed information concerning the progress of the investigation, and not simply state, "Investigation Continues."

b. If investigative jurisdiction of a DoD Hotline allegation is referred to another investigative agency, i.e., FBI, ATF, IRS, MPI, Provost Marshal, etc., the responsible USACIDC field element will:

(1) Submit a DoD Hotline Progress Report detailing the circumstances surrounding the referral and maintain liaison with the agency to which the investigation was referred.

(2) Submit a DoD Hotline Progress Report to HQUSACIDC every 90 days thereafter until completion of the investigation and the report of commander's action/judicial action is received. At that time, the USACIDC field element will submit a DoD Hotline Completion Report with a copy of the investigative agency's report attached as an enclosure.

c. If a USACIDC field element receives a request for an investigation regarding a DoD Hotline complaint from another agency, i.e., Corps of Engineers Security, Defense Logistics Agency Security, local Inspector General, etc., the following provisions apply:

(1) Inform the referring agency that the Hotline complaint must be returned, through channels, to the AHO. The AHO will formally task the USACIDC to conduct the inquiry, in accordance with AR 195-2.

(2) If the referring agency challenges established procedures, then a telephonic report should be submitted through command channels to CDR, USACIDC, ATTN: CIOP-CO.

(3) Sufficient information may be obtained from the referring agency to conduct a preliminary investigation to substantiate or refute the allegation(s). However, it will be made clear to the referring agency that this action does not constitute acceptance of the referral by or on behalf of the USACIDC.

(4) DoD Hotline Progress or Completion Reports are not required from USACIDC field elements until tasked to provide them by HQUSACIDC. All hotline reports will be completed in accordance with this regulation and forwarded only to HQUSACIDC. The HQUSACIDC will review the report(s) and make any distribution outside of USACIDC channels.

Appendix H
U.S. Army Audit Agency

Operations Center
Alexandria, VA
703-681-9809 DSN 761

Aberdeen Field Office
410-278-5785 DSN 298
Fax: 410-278-5912

Atlanta Field Office
404-464-0517 DSN 367
Fax: 404-464-0519

Detroit Field Office
810-574-6902 DSN 786
Fax: 810-574-6813

Europe Field Office
011-49-6134-604-600/527
Fax: 011-49-6134-604-526

Fort Belvoir Field Office
703-428-6392 DSN 328
Fax: 703-428-6517

Fort Bliss Field Office
915-568-3351 DSN 978
Fax: 915-568-6548

Fort Lewis Field Office
253-967-2111 DSN 357
Fax: 253-964-5297

Fort Meade Field Office
301-677-7741 DSN 923
Fax: 301-677-3360

Hawaii Field Office
808-438-3023 DSN 315-808
Fax: 808-438-4243

Huntsville Field Office
256-955-6262 DSN 645
Fax: 256-955-6716

Indianapolis Field Office
317-510-3883/1755 DSN 699
Fax: 317-510-3871

Korea Field Office
011-82-2-7918-6558/6866
Fax: 011-82-2-7918-4320

New Jersey Field Office
732-532-3181/3182 DSN 992
Fax: 732-532-4604

Fort Bragg Field Office
910-396-5698 DSN 236
Fax: 910-396-2960

Fort Carson Field Office
719-526-3025 DSN 691
Fax: 719-526-7937

Fort Hood Field Office
254-287-7721 DSN 737
Fax: 254-288-5637

Fort Huachuca Field Office
520-538-0970 DSN 879
Fax: 520-538-7096

Fort Knox Field Office
502-624-7240/7832 DSN 464
Fax: 502-624-2681

Fort Lee Field Office
804-734-1377/1841 DSN 687
Fax: 804-734-1239

Philadelphia Field Office
215-897-5201/5202 DSN 443
Fax: 215-897-5207

Rock Island Field Office
309-782-1188 DSN 793
Fax: 309-782-1186

San Antonio Field Office
210-221-2151 DSN 471
Fax: 210-221-2148

Savannah Field Office
912-352-6103/5406 DSN 971
Fax: 912-352-6812

St. Louis Field Office
314-260-2023/2002 DSN 490
Fax: 314-260-2032

TRADOC Field Office
757-727-3611 DSN 680
Fax: 757-727-3529/5889

Appendix I
Defense Contract Audit Agency

Regional Office Address

Central Region
6321 East Campus Circle
Irving, TX 75063
Phone: 972-753-2513

Eastern Region
2400 Lake Park Drive, Suite 300
Smyrna, GA 30080-7644
Phone: 404-319-4400

Mid-Atlantic Region
615 Chestnut Street, Suite 1000
Philadelphia, PA 19106-4498
Phone: 215-597-7451

Northeaster Region
59 Composite Way, Suite 300
Lowell, MA 01851-5150
Phone: 978-551-9710

Western Region
16700 Valley View Ave., Suite 300
La Mirada, CA 90638-5833
Phone: 714-228-7001

Appendix J
Presentations to Prosecutors

a. Frequently the economic crime investigator will be the individual presenting the case to the civilian prosecutor (AUSA) for determination of subsequent litigation (both criminal and civil). In such instances, the investigator must remember that the prosecutor's time is limited and, therefore, the presentation of the case must be succinct as well as comprehensive. The investigator must also consider that his personal appearance and manner before that prosecutor will influence him as much as the actual case material in the determination of prosecutive merit.

b. The following guidelines for case presentation are provided:

(1) The basic product: Whether the investigation is complete or not, the investigator should be sure that he has gathered as much evidence as possible, within the limits of his resources, before he goes to the prosecutor. In some cases, the investigator is quite able to present a complete package to the prosecutor, which the prosecutor will be able to reshape to make his own case. While the prosecutor will frequently wish follow-up on some line of investigation, it is important that no obvious line of inquiry be omitted without clear justification. The investigator must be able to demonstrate clear awareness of the legal elements of the case and have admissible, competent, and persuasive evidence on each such point.

(2) Preparing a package for a prosecuting attorney: The investigator must be able to present in written form and organized in a way that permits efficient access to all information and evidence important to the case. Even the best case is likely to be declined if it is poorly organized and presented (whether in writing or orally). It is the investigator's responsibility to organize the material to enable the prosecutor to make his decision; it is not the prosecutor's responsibility to exhaustively examine papers and question the investigator to determine what should have been clearly presented to him in the first place.

(3) Guidelines for preparing a comprehensive package: The following outline is a guide for the preparation of a comprehensive report for presentation to a prosecuting attorney. In each investigation, depending upon the case complexity and the particular organizational arrangement with the prosecuting attorney, the investigator should be able to select those elements of the outline which are applicable to the particular case. In preparing reports, the investigator should carefully and explicitly distinguish between his suppositions and the facts he has established by investigation.

Guidelines for preparing a comprehensive package for a prosecuting attorney

a. Introductory summary. A brief narrative which explains:

(1) The type of offense

(2) How it came to the attention of the USACIDC

(3) Period of operation

(4) Name, fictitious name, company name, etc.

(5) Evidence of prior criminal activity

(6) Whether rights warning was administered

(7) Type and amount of loss to U.S. Government

(8) Possible statutes (criminal, civil, administrative) which were violated

b. Description of proposed defendants. A standard identification record may be used, which contains at least the following:

(1) Name

(2) Alias

(3) Addresses (home and business)

(4) Physical description

(5) Date/place of birth

(6) Occupation/employers

(7) Associates/accomplices

(8) Prior record

(9) Identification of those who have cooperated or might cooperate with the prosecution

c. Description of offense. A detailed exposition of all pertinent data concerning the who, what, when, where, why and how of the offense from its conception

through its perpetration. For example, for each occurrence, to the extent possible, describe:

(1) How was the offense conceived?

(2) Who executed it? Who played what parts?

(3) Where it was in operation?

(4) How long was it in operation?

(5) What was the nature of the fraud and offense, the type of merchandise, service, or trickery involved?

(6) What was the specific loss to the U.S. Government?

(7) Any information which will provide the prosecuting attorney with a firm comprehension of the magnitude, nature, and characteristics of the offense.

(8) A Proof Analysis Work Sheet will be used (see figure J-1) and included as an exhibit in the final ROI.

d. Results of investigation. A narrative description containing the evidence which may possibly be used for development of proof of misrepresentations, fraudulent intent, or other essential elements of the statutes violated. Include:

(1) Any occurrences which might lead to a conclusion of criminal intent. To this should be attached any diagrammatic outlines of the fraud/offense which may have been prepared.

(2) When applicable, each major misrepresentation, false statement, pretense or promise, or conspiracy which the defendants entered into or used in obtaining money or property from the U.S. Government.

e. Possible evidence

(1) List of witnesses, (including cooperating subjects of the investigation) addresses and telephone numbers.

(2) Oral, documentary and physical evidence associated with each witness.

(3) How the evidence was obtained (through interview, surveillance, etc.).

f. Other agencies involved. A brief description of the involvement of other government, law enforcement or private agencies.

Appendix J
Presentations to Prosecutors

PROOF ANALYSIS WORK SHEET

ELEMENTS OF PROOF CORROBORATING EVIDENCE

1. Subject made statement
 1. Exhibit 4, invoice 14897, 1 April 1985, requesting payment for 25 widget kits.

2. Statement was false
 2. a. Exhibit 25, defective widget kit.
 b. Exhibit 10, USACIL report reflecting widgets are defective.

3. Subject knew statement was false
 3. a. Exhibit 8, statement of Tom Jones, Govt. inspector, indicating contractor knew manufacturing process was inadequate.
 b. Exhibit 9, MILSPEC A1422C, detailing how widgets were to perform, contained in paragraph 12C, contract DAA112.
 c. Exhibit 6, statement of John Cougar, Corp. Engineer, who details manufacturing process actually used, which does not conform to Exhibit 9, and that Bill Smith, Corp., VP, for production, told him to use the non-conforming process.
 d. Exhibit 13, statement of Bill Smith, who admits directing the non-conforming process.

4. False statement was material
 4. a. Exhibit 4, DD Form 250, Receiving Report, reflecting 25 widget kits were delivered to Fort Apache.
 b. Exhibit 14, Govt. voucher 15267, reflecting payment of $175,000 to Corp. for providing widget kits.

5. Statement was used in matter within
 5. Exhibit 1, U.S. Army contract DAA112 awarded U.S. Army jurisdiction to Corp.

Figure J-1. Proof Analysis Work Sheet

Appendix K
Subpoena Documentation

SAMPLE PERSONAL RECORDS SUBPOENA ATTACHMENT

1. Any and all originals or legible copies when originals are not available of the following documents (and copies thereof made before service of this subpoena), in your possession or subject to your control, for the period (insert time period desired):

a. Retained copies of your federal, state, and local income and other tax returns filed by you for the years (insert years desired), and work papers used in the preparation of such returns.

b. Retained copies of any federal, state, and local income and other tax returns filed by any corporations and partnerships in which you have or had a financial interest during the years (insert years desired), and work papers used in the preparation of such returns.

c. All records in any way relating to any bank account maintained by you or over which you were a signatory, or in which you have a financial interest (including: (a) checking account statements, cancelled checks, checkbooks, check stubs or registers, check vouchers, and deposit slips; (b) all savings account records; (c) all records of loans made or received; (d) all records of certificates of deposit and other time deposit items purchased or redeemed; and (e) records of all safe deposit boxes).

d. All records of purchase, ownership, and sale of stocks, bonds and other securities either made by you or by anyone else on your behalf (including securities account statements, margin account statements, checks, check stubs, deposit slips , correspondence, notes and memoranda).

e. All records of credit card or other charge account purchases made by you or by anyone else on your behalf.

f. All records of reimbursement of expense received by you from any source.

g. All records of inheritances, bequests, and other such gifts received by you.

h. All records of insurance claims made by you, for, or on account of any death or any injury to person or property (including insurance policies, binders, riders, claims, claim forms, medical reports, investigative reports, checks, deposit slips, correspondence, notes, and memoranda).

2. Any and all original documents (and copies thereof made before service of this subpoena, in any way relating to any transaction between you, and any of the following individuals and entities, or any entity of which any such individual is an owner , officer, director, manager, partner, or employee, during the period (insert time period desired):

(insert names of individual and entities)

3. (Other paragraphs, as appropriate, describing subpoenaed materials).

SAMPLE PARTNERSHIP RECORDS SUBPOENA ATTACHMENT

Any and all originals of the following documents (and copies thereof made before service of this subpoena), in your custody or subject to your control, for the period (INSERT TIME PERIOD DESIRED):

1. Name and address of all individuals and/or entities that now have or have ever had any direct financial or ownership interest in the (INSERT NAME OR PARTNERSHIP) (hereinafter referred to as the "partnership").

2. Copies of partnership agreements including any amendments thereto, and all minutes or other records of partnership meetings.

3. Retained copies of all federal, state, and local partnership tax information returns filed for the years (INSERT YEARS DESIRED), and work papers used in the preparation of such returns.

4. All banking records (including (a) checking account bank statements, cancelled checks, checkbooks, check stubs or registers, check vouchers, and deposit slips; (b) all savings account records; (c) all records of loans made or received; (d) all re cords of certificates of deposit and other time deposits purchased or redeemed; and (e) records of all safe deposit boxes).

5. All partnership ledgers and journals (including the general ledger, cash receipts journal, sales journal, cash disbursements journal, voucher register, and any other ledgers and journals maintained by the partnership).

6. All records of capital contributions and cash or property withdrawals from any and all partners' capital accounts.

7. All financial statements prepared by or on behalf of the partnership.

8. All vendor invoices and statements of accounts, customer billing invoices and statements of account, vouchers, and any other records used in determining gross income, deductions, and the balance sheet reflected on the partnership tax information returns.

SAMPLE CORPORATE RECORDS SUBPOENA ATTACHMENT

Any and all originals of the following documents (and copies thereof made before service of this subpoena), in your custody or subject to your control, for the period (INSERT TIME PERIOD DESIRED):

1. All corporate ledgers and journals of the (INSERT NAME OF CORPORATION) (hereinafter referred to as the "corporation") (Including the general ledger, cash receipts journal, sales journal, cash disbursements journal, voucher register, and any other ledgers and journals maintained by the corporation).

2. All banking records of the corporation (including (a) bank statements, cancelled checks, checkbooks, check stubs or registers, check vouchers, and deposit slips; (b) all savings account records; (c) all records of certificates of deposit and other time deposits purchased or redeemed; and (d) records of all safe deposit boxes).

3. All records of loans received and made by the corporation, including any and all correspondence related to such loans.

4. All corporate minutes and/or other records of recordings, of any kind whatsoever, of corporate meetings and the corporate charter and bylaws, including any revisions and amendments thereto.

5. All financial statements prepared by or on behalf of the corporation.

6. All retained copies of federal, state and local tax returns for the years (INSERT YEARS DESIRED), and work papers used in the preparation of such returns.

7. Corporate stock ledgers.

8. All vendor invoices and statements of accounts, customer billing invoices and statements of account, vouchers, and other records used in determining gross income deductions, and the balance sheet reflected on the corporate income tax returns.

9. All records in any way connected with the acquisition or sale of real and/or leasehold property by the corporation either improved or unimproved (including purchase contracts, settlement sheets, contracts of sale, deeds, notes, mortgages, deeds o f trust, leases, correspondence, memoranda, and notes of meetings and/or telephone calls).

10. All records of tangible and intangible personal property legally or equitably owned by the corporation (including, for example, stock and bonds).

11. All records relating to corporation construction loan agreements and mortgages, draws, fees, and permanent financing commitments and mortgages (including all correspondence, memoranda, notes, and other materials relating thereto).

12. All personnel files of current and former employees and consultants.

13. All U.S. Information Returns (Form 1096 and 1099), Employer's Quarterly Federal Tax Returns (Form 941), and Employer's Annual Federal Unemployment Tax Returns (Form 940) filed by the corporation.

14. All travel and entertainment records.

15. All records of commissions, rebates, discounts, bonuses, gifts, or other payments made by the corporation to any person or entity who is not an officer, director, manager, member, or employee of the corporation.

16. All agreements, contracts, memoranda of understanding, and other such documents, reflecting or containing any agreement between the corporation on the one hand, and any individual as an owner, officer, director, manager, partner, or employee, on the other hand:

(Insert names of individuals and entities)

SAMPLE BANK SUBPOENA ATTACHMENT

Any and all original documents (or microfilm copies where originals are not available), in the bank's custody or subject to its control, that in any way relate to any of the following persons and entities, or to any checking, savings, or loan account s for, by, or to, or on behalf of them either individually or on behalf of, in trust for, or in combination with any other person or entity for the period (insert time period):

(Insert list of names of persons and entities whose records are subpoenaed)

Including, but not limited to the following documents:

1. Signature cards of all accounts.

2. Monthly checking statements.

3. Copies of all cancelled checks.

4. Transcripts of savings accounts.

5. Copies of deposit slips for checking and savings accounts, and deposit items to which those slips relate.

6. Loan records, including collateral loan records.

7. Loan ledger sheets.

8. Safe deposit box records of access.

9. Financial statements and credit reports.

10. Copies of promissory notes.

11. Mortgage records and applications.

12. Copies of certificates of deposit.

13. Investment and/or custodian accounts.

14. Records of purchase of bearer bonds.

15. Safe keeping register records.

16. Records of transfer of funds by wire or collection.

17. Receipts of delivery of securities.

18. Copies of application for purchase of manager's checks, cashier's checks, and/or treasurer's checks, together with the checks that were purchased.

SAMPLE ACCOUNTANT'S RECORDS SUBPOENA ATTACHMENTS

Any and all original documents (and copies thereof made before service of this subpoena), in your custody or subject to your control, whether owned by you or by anyone else, that in any way relate to the following persons and entities, whether individually or in combination with any other person or entity, for the period (insert time period desired):

(Insert names of persons and entities whose records are subpoenaed)

including but not limited to the following materials: federal and state tax returns (including retained copies thereof), work papers, financial statements, check spreads, audit reports and other records of financial examinations, correspondence, memoranda, notes, and copies of documents prepared for filing with any agency of the federal government, any state or local governments, or any bank or other financial institutions.

SAMPLE STOCKBROKER'S RECORDS SUBPOENA ATTACHMENTS

Any and all original documents, in your custody or subject to your control, that in any way relate to the following persons and entities, whether individually or in combination with any other person or entity, for the period (insert time period desired):

(Insert names of persons and entities whose records are subpoenaed).

including, but not limited to, the following materials: applications for accounts, account statements and other records of securities purchased and sold (including records of margin accounts and cash proceeds kept or maintained by you, for, or on be half of any of the individuals or entities described above), stock ledger sheets, checks, check stubs, deposit slips, correspondence, notes, and memoranda.

Appendix L
Suggested Guide for Preparing a Memorandum of Understanding for Drug Suppression Operations

MEMORANDUM OF UNDERSTANDING BETWEEN
FORT SMITH RESIDENT AGENCY, USACIDC
AND
THE PROVOST MARSHAL FORT SMITH, TX 55555

SUBJECT: Fort Smith Drug Suppression Team (DST) Operations

1. REFERENCES:

a. AR 190-30, Military Police Investigations, authorizes the employment of MPI on DSTs.

b. AR 195-2, Criminal Investigation Activities, authorizes the execution of MOUs between USACIDC and the Provost Marshal (PM).

c. CIDR 195-1, CID Operations, authorizes and encourages combined drug suppression operations, describes MOUs, their format and specific requirements to be contained in the MOU. It also gives policy and guidance on the Criminal Investigation D rug Suppression Program.

2. PURPOSE. This Memorandum of Understanding (MOU) delineates investigative and support responsibilities pertaining to the suppression and investigation of narcotic offenses and those marihuana and dangerous drug offenses involving distribution and for the possession of marihuana or dangerous drug in distribution quantities, as defined.

3. OBJECTIVE. To establish a CID and MPI Drug Suppression Team to reduce the availability and use of drugs within the Fort Smith military community.

4. DEFINITIONS. The title PM as used throughout this MOU also applies to the position of Security Officer and Commander, Law Enforcement Activity.

5. RESPONSIBILITIES:

a. The Fort Smith Resident Agency, USACIDC, will establish or provide (list support provided such as):

(1) A drug suppression program in accordance with AR 195-2 and CIDR 195-1 to combat the drug threat at Fort Smith.

(2) Office space.

(3) Commercial design vehicles and covert vehicles.

(4) Station property such as desks, typewriters, etc.

(5) Non-standard weapons as required for DST personnel.

(6) Telephones.

(7) CID funds for DST operations.

(8) Drug test kits.

(9) Gasoline for all vehicles used by DST.

(10) Rations, quarters, and military justice (applies only to attached personnel or as agreed upon by PM and the CID supervisor).

b. The Fort Smith Resident Agency, USACIDC, will also:

(1) Process all sequence number actions, initial reports, status reports, and final reports of investigation.

(2) Process administrative actions for CID assets.

(3) Submit reports as required to action commander.

(4) Deposit and secure all evidence acquired by the DST in the Fort Smith Resident Agency Evidence Depository.

(5) Assume property accountability and responsibility for rental vehicles.

(6) Provide training to all DST personnel.

c. The Provost Marshal, Fort Smith, TX, will provide the following support (list support provided such as):

(1) Typewriters.

(2) Weapons for MPI or MP personnel.

(3) Hand irons for MPI or MP personnel.

(4) MP radios and chargers.

(5) Individual training (i.e., Skills Qualification Test, Common Task Testing or Training, etc.)

d. Investigative Responsibility. The DST will be responsible for investigation of possession of marihuana and dangerous drugs in "distribution quantities" as outlined in appropriate regulations or as agreed upon by the PM and CID commander. The following examples are provided:

(1) Dangerous drugs in a quantity of 20 or more user units (tablets, capsules, etc.) or loose powder weighing .5 gram or more.

(2) Hallucinogenic drugs in quantities of 10 or more user units or any amount in powder form.

(3) Marihuana weighing 30 grams or more.

(4) Hashish weighing 10 grams or more.

(5) The above quantities or amounts apply to a single individual and not to the aggregate possession of more than one individual.

e. Command and Control. The Special Agent-in-Charge, Fort Smith Resident Agency, is responsible for the DST. The senior accredited special agent member of the DST will be designated as the team chief. All other personnel employed with the DS T will be under the direct control and supervision of the team chief.

6. PROCEDURES:

a. Organization. The DST will be organized as follows:

(1) The senior accredited special agent will be designated as the team chief.

(2) Additional CID agents as team members.

(3) Military Police Investigators, MOS 95BV5, will be provided by the PM, Fort Smith, TX. (The specific numbers of CID agents and MPI and MP should be stated).

b. Briefings. The PM, or his representative, will be briefed (weekly, bi-weekly, or monthly as agreed upon in this MOU) by the Special Agent-in-Charge, Fort Smith Resident Agency, or his representative concerning completed, on-going or planned operations of the DST. Additional briefings will also be provided to the PM upon request or initiative of the Special Agent-in-Charge, Fort Smith Resident Agency. Briefings for installation officials and action commanders of subjects of investigations will be conducted by the Special Agent-in-Charge, Fort

Smith Resident Agency. Briefings to the post Chief of Staff will be accomplished jointly by the Special Agent-in-Charge, Fort Smith Resident Agency, USACIDC, and the PM, Fort Smith, TX.

c. Training. All personnel assigned to the DST will successfully complete the formal training course provided by the Fort Smith Resident Agency prior to engaging in drug suppression operations. This training will be as specified in the Fort Smith Resident Agency Drug Suppression SOP.

d. Tenure. Special agents, MPI, MPs, and non-MP personnel will normally perform duties with the DST for a period of one year. Considerations may be given to providing personnel for a period less than, or longer than, one year in the event of military necessity and as agreed upon by both the PM and CID commander. If any MPI/MP/non-MP personnel are removed from the DST for cause, appropriate documentation and notification will be provided to the PM/appropriate unit commander for necessary action.

e. Attachment Orders. Personnel of the 222d MP Co, performing duty with the DST on official orders to the Fort Smith Resident Agency, USACIDC, will be attached for duty, training, and performance evaluation reports for a period of one year. (Applicable only when personnel are to be attached).

f. Personnel Ratings. All members of the DST will be rated by the team chief, DST, and reviewed by the Provost Marshal. Those personnel working DST duties not assigned or attached on orders will be rated by their normal rater with performance input provided by the DST team chief.

g. Adjustments. Signatures to this memorandum acknowledge that USACIDC and MP personnel considerations or fluctuations in the workload of the DST may require personnel adjustments. Such adjustments will be made pursuant to coordination and agreement between the signatories.

7. COORDINATION. This MOU was coordinated with the Fort Smith Installation Commander and Staff Judge Advocate.

8. EXPIRATION. This Memorandum of Understanding will become effective upon signing by both parties and remain in effect for a period of one year at which time it must be renegotiated.

BRIAN C. NOVICE	JAMES S. OSSORIO
CW3, USA	Colonel, MP
Special Agent-in-Charge	Provost Marshal
(DATE)	(DATE)

Appendix M
A Guide to Source Handling

M-1. General

a. Registered source handling is one of the most important aspects in a criminal investigation. It is based primarily on a one-on-one relationship. This unique relationship makes it difficult to teach handling in a classroom or learn source handling solely from available literature. Valuable information can be obtained from FM 19-20; however, neither this manual nor other publications outline, in detail, some of the daily pitfalls and "booby traps" handlers encounter. This information should be viewed as a guide and may be modified by the individual agent to meet specific objectives.

b. Procedures will depend on the needs and wants of the agent, the character of the source, and the type of criminal investigation involved. Modifications may also be based on peculiarities of specific operations, such as geographic location, type of troops involved, primary installation functions or the availability of illicit drugs or other crime conducive conditions. More importantly, such modification will depend on the character, personality and experience of the agent handling the source.

c. CID agents become more proficient by using sources to acquire information and solve crime. New agents, or ones with limited experience, can often see the successes of agents with productive sources. Although sources are more commonly used in drug suppression the general and economic crime areas should not be overlooked. Just as a proactive drug enforcement program cannot be totally successful without the use of sources, proactive general and economic crime efforts are also impacted by the use of sources.

M-2. Source recruitment

a. The recruitment stage is the most critical phase of an agent's relationship with a source. Criteria for selection of a source is covered in FM 19-20, chapter 6.

(1) There are numerous areas from which sources can be drawn. Most often, source recruitment procedures can be handled in an overt manner, with the handler being identified as an agent from the beginning. An agent may use the fraud awareness briefing or drug briefing to make an initial entry into a crime conducive area that might not otherwise be readily accessible. This direct

approach does not present a problem when dealing with individuals who have volunteered to work as sources, or with those who have been apprehended by law enforcement authorities and are now working for the law enforcement agencies. This approach should not cause a problem when an agent's investigative activities are overt and there is no possibility of compromising an undercover role or mission. Where a direct recruiting technique is used, the primary security concern is protecting the potential source's status.

(2) When an agent is operating in a covert capacity, any approach to recruit a source may present a threat to the agent's covert status or to the covert operation.

(a) Direct approach. Covert agents must consider the possibility of a source working for law enforcement and the criminal element simultaneously, or a source cooperating with criminal suspects at some future time. These possibilities and their effect on the mission should be considered prior to recruitment. It may be appropriate initially to recruit a source through another agent. The recruiting agent's identity as a law enforcement official should be known or he should be in a position where his compromise would not jeopardize a covert mission. After satisfactory completion of reliability tests and background checks, the source can be transferred from the recruiting agent to the covert handler.

(b) Indirect approach-unwitting registered source. In a specific mission, it may become necessary to employ a source while the covert agent poses as a criminal. This procedure requires extreme caution and is highly sensitive. Where the source believes he is employed by a criminal, rather than an agent, certain modifications in normal source handling are necessary. It is not likely that full identification can be obtained, except through indirect methods. Partial identification on the CID Form 20 (source data card) is appropriate and can be as brief as a nickname and description. In these instances, a covert photograph should be obtained if possible. Bonuses and expense reimbursements can be paid to this source from .0015 funds IAW AR 195-4. Whenever possible, payments of .0015 funds to unwitting sources should be witnessed by another agent (or investigator) and recorded on the statement prepared by the handler documenting the transaction. If the source is unwitting, the handler will record full details of the payments in the source file and indicate on a justification document that the source is unwitting. The use of unwitting sources is not limited to areas of illicit drugs or general crimes, but can also be extremely useful in the economic crime area.

b. Initial interviews and contacts. This phase of the handler/source relationship is of paramount importance in establishing rapport and appropriate courses of action. Properly handled, initial meetings can do much to preclude many pitfalls encountered by agents after they have recruited a source. During initial interviews, the agent should accomplish the following:

(1) Determine source motives. Even potentially dangerous motives can be successfully exploited providing they are identified at an early stage in the handler/source relationship. Examples of source motivation are:

(a) Leverage. The source is looking out for his best interest, i.e., less punishment for an offense he has committed.

(b) Money. The source is looking for monetary gain.

(c) Revenge. The source wants to get even with someone.

(d) Concern Citizen. The source feels an obligation to society.

(e) Egotistical motives. The source wants to feel important. Here the ego of the source is enhanced by informing to the police.

(f) Fear. Self-preservation is the first law of nature. Fear could be for any number of reasons: Fear of arrest or indictment by the police, fear of reprisals, fear of being "pushed out," or fear of blackmail.

(g) Other. To many, the thrill of detective work is overwhelming. Once started, the person wants to continue. To some, they may condone one type of crime, such as housebreaking, but not crimes of violence. This type may be more than willing to assist the police in apprehending violent criminals. Another type is the source who will pass on information to the police in hopes that it will provide him with an advantage. He informs on others in an effort to eliminate competition. You should be aware that there are those who may "offer" to inform in an attempt to learn what is known about their own activities, or to try and divert suspicion from themselves. They may offer to inform in order to "get close" to the police to learn of any danger to themselves or their associates.

(2) Determine the geographical area of usefulness. This includes consideration of areas normally frequented, access to transportation, willingness to travel, and so forth.

(3) Identify the extent of the source's association with criminal elements at the time of recruitment. If the source is a volunteer, he may have no connection with criminal suspects and may need specific guidance in targeting and infiltration. Conversely, some sources may be too close to criminal elements. This requires that the handler provide detailed instructions to the source and conduct stringent surveillance of his activities.

(4) Analyze the most appropriate area of potential usefulness of the source. This may include the crime area with which the source is most familiar, for

example, a high-crime location on or off an installation, the source's general peer group, or his own military organization.

(5) Determine the source's knowledge about the area where he is to be used. See if he can provide specific information about a particular activity within an operation and if he has the ability to identify criminality.

(6) Identify any potential conflicts which might adversely affect a military source's usefulness. For instance, a source's first sergeant may have a strong dislike for the individual due to the source's performance as a soldier. Consequently, the source's freedom of movement and usefulness may be severely impaired by controls and disciplinary measures imposed by his unit. Another concern is the individual who is suspected of working for the USACIDC. Such problems can be successfully overcome by appropriate "camouflage" techniques, but must be considered prior to use of a source.

(7) Determine if anyone is aware or suspects that the source desires to work for and is being interviewed by the USACIDC. Often the handler will find that the girlfriend or boyfriend, other close friends, relatives, unit commanders, and first sergeants are already inadvertently in positions to compromise the confidential status of the source. Under these circumstances, the source's potential usefulness must be weighed against the risk of compromise.

(8) Determine the degree of initial reliability by means of the following criteria:

(a) Detect criminal history by CRC name checks, local police checks, and criminal intelligence files.

(b) Determine the credibility of a potential source. Often, USACIDC sources may have worked as a source in the past. They may have provided useful, reliable information to other agents or police agencies. They may have worked for their own unit commanders or first sergeants. A simple confirmation, through these sources, might establish sufficient reliability for search warrant purposes with "walk-in" or "first time" sources.

(9) Evaluate the reliability of a source, during the earliest stages of recruitment and continually throughout the period of active targeting of a source.

c. Establish and maintain the handler/source relationship.

(1) The handler should remain totally in control of the situation when talking to a source and maintain full supervision over all the source's USACIDC-related activities.

(2) A Declaration of Understanding may not be appropriate for certain types of sources. When used, the contents of this form should first be explained to a source by the handler. The source will then read, initial and sign the form. It will then be placed in the source's file.

(3) The handler should ensure the source understands the limits and extent to which his name will be kept confidential. This may include an explanation of the use of code names and numbers and an explanation of the possible legal necessities for revealing the name of a source.

M-3. Registered source training.

Questioning during the recruitment process will determine the extent of the source's knowledge regarding criminal suspects, elements, and activities. The source may know very little about this type of activity and need training before he can be properly used. The following instructions should be given to potential sources before they start working for the USACIDC:

a. How to gather criminal intelligence, to include:

(1) Full name or part thereof.

(2) Description (male; Cauc; 20 yrs; 170 lbs, 69 in; medium build; long brown hair; bushy mustache; wearing ...).

(3) If military, the unit and where he or she works in the unit.

(4) If civilian, where employed, etc.

(5) Off and on-post addresses.

(6) Description and license number of vehicle, if any involved.

b. When uncovering a location involved in criminal activities or the suspect's residence:

(1) Pinpoint exact address and describe fully.

(a) Describe exterior of location.

(b) Describe interior premises (with sketch) including doors, windows, bathrooms and exact locations of any evidence.

(2) Identify all occupants of the location.

(a) Individually.

(b) Their relationships to each other and the criminal enterprise.

(c) Who owns or rents the location or dwelling? If a house or apartment, it can be stated generally, "This is a nice place, what does it cost a month?" The individual who pays the rent or mortgage is likely the one who will answer this question. There can be further questions asked under the pretext that you are searching for a house/apartment yourself.

(d) Extent of criminal involvement.

(e) Methods of operation.

(f) Locations where criminal activities are conducted.

(g) Suspect's criminal associates.

c. How to describe and recognize stolen property, including:

(1) Where the stolen property is being stored.

(2) Where feasible, obtain serial numbers and full descriptions of suspected stolen property on the premises.

d. If the suspect is actually observed engaging in criminal activities, how to identify the following:

(1) Who participated?

(2) What did the suspect(s) do?

(3) When?

(a) Times.

(b) Dates.

(c) Last time. (This should be recent for a search warrant, etc., by the CID).

(4) Where did the criminal activity occur?

(5) How was it done?

(6) Why was it done?

(7) Will the source be compromised by any actions taken based on the information provided?

e. Time considerations from observation to reporting:

(1) The USACIDC cannot act on information which is not current.

(2) If the information involves a person committing criminal acts, it must be reported immediately for the USACIDC to take appropriate action.

f. Describe any vehicles involved in the criminal activities?

g. Describe any weapons which suspects might use in the event of their apprehension or a search of their residence or place of business?

h. Describe any plans that were overheard regarding escape routes or methods of hiding or destroying contraband items in the event of an apprehension or search.

i. Extreme caution must be used when making observations. Ensure that others have also observed the same activities, etc., to cover possible future compromise. Any possibility of compromise to identity or safety should be immediately reported to the controlling agent.

j. Organize information in chronological order including all known details in order to provide a complete picture of what has occurred. This is particularly important for time sensitive reports.

k. Source's actions during apprehensions.

(1) Prior briefings.

(2) Signals during operations.

(3) Actions of source during meetings with criminal suspects.

(4) Actions of source following apprehensions.

(a) Meeting with handler immediately thereafter.

(b) Debriefing and possible statement.

l. Laws (as applicable).

(1) U.S. military vs. Federal, State and local laws.

(2) Foreign laws.

(3) Entrapment and conspiracy laws (in detail).

(4) Criminal responsibility and civil liability.

m. Evidence handling.

(1) Prevention of contamination.

(2) Methods by which a source should handle contraband when necessary.

(3) Chain of custody.

n. Limitations of law enforcement agencies (provide only necessary information, particularly where the source is a known prior offender).

(1) Surveillance limitations (vehicle problems, communications, locations for meetings which cause surveillance problems, etc.).

(2) Jurisdictional limitations.

(a) Military connection

(b) Military vs. civilian police agencies.

(c) Foreign law enforcement agencies.

o. Limitation .0015 fund applicability.

(1) Payment of bonuses.

(2) Reimbursement of actual expenses (limitations).

M-4. Source handling suggestions.

A significant percentage of sources have been involved in drug or other contraband investigations. This type of covert operation, by its nature, usually requires direct contact or negotiation with criminal suspects and provides a continual flow of information. Such operations create an atmosphere that lends itself to the use of sources in a highly controlled manner. Although sources in other crime areas require different sets of control measures, the basic principles apply to the handling of sources in all crime areas. Individual sources can be used simultaneously in more than one crime area and their activities can easily

cross from one crime area to another. Some handling techniques which have proven to be effective are listed as follows:

a. Camouflage techniques. These techniques are measures to protect a source's identity before, during and after a covert operation and to reverse any suspected possibility of compromise to a source. If suspects are apprehended during a covert operation, and the source is present, thought should also be given to apprehending the source. The source should be processed normally, then released later under an appropriate pretext. Make certain all other suspects are questioned regarding the alleged criminal activities of the source.

b. Familiarity.

(1) Familiarity between the handling agent and the source.

(a) The agent must remember that he should remain separate from the source in all but professional situations, so as to maintain control and mission effectiveness.

(b) The handling agent must be concerned for the source's personal and military-related needs and requirements, such as the following:

(1) Timely payment of bonuses and/or reimbursement of justifiable expenses.

(2) For military sources, their paycheck, mail, quarters, medical requirements, and NCOERs, are received promptly.

(3) Personal affairs, such as legal problems, domestic problems, and family member schooling.

(4) Protective measures, such as maintaining confidentiality of the source's identity and the care in the choice of meeting locations, etc., should be exercised at all times.

(c) Sources will require frequent work-related contacts, and continual motivation by means of challenging assignments, praise, monetary reward, or whatever method is most effective. During each contact, the handling agent must be constantly mindful of the continuing employer/employee relationship.

(2) Familiarity between sources. Normally, sources should not be familiar with, or even know, the identity of other sources. Occasionally, this may happen or may be necessary, but familiarity between sources should never be commonplace. A few of its dangers are listed below:

(a) The possibility of source compromise is increased significantly, as it is often the case that one of any group of sources will later turn back to criminal enterprises or be compromised himself. This situation may lead to t he compromise of other sources by simple association with him.

(b) Familiarity promotes petty jealousy and disproportionate competition among sources. This can lead to sources lying to the handler about suspects and criminal activities to enhance their personal reputation.

(c) Sources are able to compare treatment, bonuses, etc., which may lead to unwanted conflicts and problems.

(d) Sources can exchange case-related information which may compromise certain operations or provide them with too detailed a picture of CID operations on the whole.

(3) The team-concept in source handling. Source teams of two males, man and wife, male and female, or two women can be useful and effective where the particular circumstances of a covert operation call for such extreme measures. Stringent supervision and constant control measures are essential in such cases. For this reason, they should be limited to short-term operations.

c. Protection of the Handling Agent. Sources have been known to act in peculiar ways towards their handlers. Their motives for such unusual actions may be something as apparently insignificant as a few strong words shouted in anger at them by the handler, or even common jealousy. For whatever motive, they may turn against the handler and seek revenge. For instance, sources may accuse handlers of the opposite sex of making sexual advances. The disgruntled source may allege that his handle r has committed illegal, unethical or immoral actions. To protect themselves, special agents should consider the following:

(1) Document all meetings with sources for later reference, even when they do not have a direct bearing on an investigation.

(2) Have a witness or at least a back-up surveillance during meetings with a source of the opposite sex. A back-up surveillance is a good policy when meeting with all sources.

(3) Conduct frequent tests and surveillance of sources. These activities assist agents in evaluating source reliability as it applies to specific missions. Additionally, it assists in evaluating the source's general reliability in regard to the ongoing agent/source relationship.

(4) Know where sources are and what they are doing by means of control procedures. The amount of problems a source will cause his handler are usually

inversely proportional to the quality and degree of control exercised by the handler. The higher the degree of control, the less the problems.

(5) Get receipts for payments rendered, if possible, or in the case of unwitting sources, always have a witness present or observing the payment. Under no circumstances should a source be requested or required to sign a blank receipt.

(6) Register sources with source control officers and the source register officer. If a problem arises where an accusation is made against an agent by a source, it will be in the agent's favor to have already registered the source and documented his activities, rather than the source coming as a surprise to the management level. Should the agent or source die or become in any way incapacitated, there is a record of activities on which to continue the investigations or initiate an investigation.

(7) Short of mission necessities, never do anything or appear to do anything with or in front of a source which you as an agent would not want to be made public knowledge at some future date.

(8) Never say anything to a source which if passed to criminal elements could not adequately be covered through camouflage techniques or other methods.

d. Shotgun pattern vs. targeting. The shotgun pattern is a tactic in which the handler instructs a source to go out and "do good and fight evil." The source then targets on locations, groups, or individuals at will. Experience has shown that this amount of latitude can quickly become uncontrollable. The source will soon be running the case and may even be making assignments and allocating resources. At best, the source with this kind of free hand will be setting the direction of investigations in which he develops the initial leads. The source should be assigned to as narrow a target area as possible, even when gathering general criminal information. This area may be as limited as one robbery suspect or one unit where a series of larcenies have occurred. Conversely, it may be as broad as an entire section of a post where a series of rapes have taken place. Whatever the scope of the target, managing a source by this technique facilitates control which is the most important aspect of the handler/source relationship.

e. "Last Minute" source operations. Invariably, sources will call handling agents and excitedly report, "Joe SMITH has a stolen rifle in his wall locker. You have to get him fast, right now, or it might be gone." This may be a good time to back-off, calm the source down, and get all of the credible information from him. More importantly, this action will facilitate the formulation of an adequate plan of action. Too often sources call in "quickie" operations and agents tend to respond too fast from fear of losing the "game." A careful plan should always be prepared and executed. The risk of moving with speed should be weighed against the possible results. It may be appropriate to let the information pass completely and give the source a stern warning to allow more lead time in the future.

f. Negotiation tactics. During the course of a source's activities for the CID, he will often become involved in negotiations with suspects for the future delivery of illegal drugs, other contraband items, or stolen property on the illicit market, etc. The following is a list of several suggested tactical moves which might be appropriate during such investigations:

(1) Do not allow the source to represent himself as the main buyer, but merely as a lieutenant or "front man." Covert agents should normally enter the negotiations as the primary purchaser.

(2) The handler should exercise rigid control of the source during negotiations with criminal elements.

(3) Do not allow the source to provide the suspects with too much information regarding the main buyer (covert agent), such as physical description, names or elaborate cover stories. The suspect needs to know only that the source represents a purchaser who has the money to conduct the transaction. This tactic prevents needless compromise of an agent based on descriptions, names, etc., and allows the latitude to insert another agent as a buyer at the last minute, if needed.

(4) Sources should not allow suspects to dictate terms regarding locations or methods of conducting transactions. Often sources will report the suspect has instructed there will be no weapons, the money must be provided first before delivery, that the transaction must take place in a secluded spot (impossible for security of the flash-roll or surveillance), he will have five bodyguards with him, etc. The suspect will advise the source that the transaction will not be conducted if all these conditions are not met. Sources, in turn, often become excited by this and feel that unless the handler is willing to comply, he (source) will lose the bonus, or whatever other incentive for which he is working. Often, a quick and agreeable response to such instructions will cause suspicion on the part of the suspects that they are negotiating with police who have no fear of being robbed or arrested. These conditions may be initially provided as a test to observe the reaction of the alleged purchaser. An optimum meeting point on terms must be agreed upon and sources must be instructed to return to the suspects with a negative response in spite of their apprehensions about losing the business and thus, their reward.

(5) Potentially dangerous sources. Some sources exhibit behavioral characteristics and actions which can alert a handling agent to potential dangers to the mission or specific covert operations and to the safety of the source, covert agents, and other law enforcement personnel involved. Handling agents should be alert for the following:

(a) A source who cannot receive and execute instructions, particularly if he is head-strong rather then merely unintelligent. Sources must know that they have a script to follow, written by the handling agent or other law enforcement personnel, and that the source does not have the prerogative to make changes in that script.

(b) A source guilty of constant procrastination. This individual will invariably make excuses why he cannot ferret out requested information or infiltrate a targeted group, suspect or location. He is wasting the handler's time.

(c) Sources who appear to be working steadily on a specific operation, and in the middle, or at the last minute drop the matter. This may be due to fear, personal problems or other reasons. In any case, if they do it once, the re is no way to guarantee it will not happen again, or on every operation.

(d) A source who constantly promises "the big man" recovery of large quantities of illicit drugs, stolen property, etc., but never delivers. This individual, unless identified quickly and terminated, can cause an enormous waste of .0015 monies and man- hours with no results.

(e) The source who plays the "agency game" by taking his information to several agencies and determining the highest bidder, or who is actually working on an investigation for more than one police agency at the same time. In such cases there may be as many as three or four separate but parallel covert investigations being conducted simultaneously against the same criminal suspect or group by different law enforcement agencies through the same source.

(f) A source who feels that he knows as much, if not more, than the handler about police procedures and techniques. He will try to run investigations and make decisions without consulting with the handler and often without the handler discovering the problem until damage has been done.

(g) The source who, for whatever motives and in spite of counseling by the handler against such actions, entraps suspects or actively provokes criminal activity. Unfortunately, the handling agent often discovers this problem only after the fact and possibly not until the suspect is brought to trial.

M-5. Remuneration guidelines

a. Expense reimbursement. Sources may be reimbursed for certain expenses. The guidelines for reimbursement are outlined in AR 195-4.

b. Bonus payments. Sources may be paid bonus payments. The guidelines for bonus payments are also outlined in AR 195-4. Bonuses should be consistent

with what would be paid by local/Federal/foreign police agencies in an area, and should not exceed such standards unless specifically and fully justified.

M-6. Importance of source program management.

A handler over a period of time develops an affinity and strong proprietary attitude toward his sources. Although no handler likes a supervisor telling him his source is nonproductive, it is imperative to have an objective, outside review of the source's activities to ensure a viable and effective source program. Consequently, each handler must continually re-evaluate his source's productivity, effectiveness, and potential to the investigative mission.

Appendix N
Control Room Standard Operating Procedures

PROTECTIVE SERVICES UNIT CONTROL ROOM STANDARD OPERATING PROCEDURES

SECTION I APPLICATION

1. PURPOSE. To establish overall policies for administration and operation of the Protective Services Unit (PSU), USACIDC, security control room during protective service missions in support of any designated principal. To provide uniformity and continuity in the operation of the security control room as the principal travels from one location to another.

2. SCOPE. This standing operating procedure applies to all military and civilian personnel tasked to support protective service operations for any designated principal.

SECTION I ORGANIZATION AND RESPONSIBILITIES

1. ORGANIZATION. The organization of the security control room at each location will vary depending on the principal, the size of the official party, the size and composition of the security force, the local threat, the type accommodations provided for the principal and his party, and other circumstances.

2. RESPONSIBILITIES. The PSU agent designated as the Mission Special Agent-in-Charge (MSAC) is directly responsible for the overall conduct of the mission.

3. DEFINITION. For the purpose of this SOP, the term "key person" refers to the Assistant to the Secretary or Deputy Secretary of Defense for Personal Security; the Senior Military Assistant to the Secretary or Deputy Secretary of Defense; the Executive Assistant or Senior Aide to the Chairman or Vice Chairman, Joint Chiefs of Staff, Secretary of the Army, Chief or Vice Chief of Staff, Army; or the MSAC.

SECTION I POLICIES AND PROCEDURES

1. SECURITY CONTROL ROOM.

a. The security control room is the command and control center for the security forces responsible for the protection of the principal. It functions as the focal point for the principal and his party for information on security and other matter s.

b. The security control room is manned at all times during the principal's visit, but only by essential security personnel. It is the terminal or monitoring point for electronic surveillance, alarm systems and security communications systems. T he security control room will be established and fully operational at least two hours prior to scheduled wheels-down.

c. Security control room personnel will be tasked with numerous and varied duties. Each task will contribute to the safety and welfare of the principal, and is therefore important. Security personnel will have no fire fighting or similar duties assigned. Such emergencies offer an excellent diversion to cover the unauthorized entrance of an assailant. Security personnel will be tasked for security related duties except as directed by the MSAC or his/her representatives.

d. The security control room is a business office which may be visited by senior representatives for the United States or host nation governments. It must be maintained in a high state of cleanliness and order and never present a cluttered or unkempt appearance.

e. The security control room is not a squad room for "off duty" security personnel, nor a lounge for members of the official party. It is the responsibility of the MSAC with the assistance of the "Trip Coordinator" on the principal's staff to ensure that only essential personnel are in the Control Room.

f. The security control room will normally be located in close proximity to the principal's suite. Therefore, noise and excessive incoming and outgoing traffic must be kept to a minimum. The volume level of communications systems in use will be tuned only loud enough to allow the duty agent to monitor transmissions. All conversations will be in moderate tones. No commercial radios, televisions or other entertainment systems will be operated in the security control room.

g. Smoking in the security control room is prohibited. The MSAC may establish guidelines to provide relief for smoke breaks for the duty agent.

h. If the duty agent cannot be relieved for meals, he/she will be permitted to take meals in the control room provided all litter is promptly removed from the room. Under no circumstances will food or beverages be charged to the control room.

i. Alcoholic beverages will not be consumed for at least twelve (12) hours prior to beginning a tour of duty.

j. Security personnel will be attired in coat and tie at all times in the security control room and will conduct themselves in a professional manner. Except in emergency situations, weapons, handcuffs, etc. will be completely concealed and not displayed for any reason.

k. Non-standard weapons (shotgun, machine pistol) may be stored in the security control room. Only agents who have been trained with these weapons within three months preceding this mission are authorized access to those weapons.

l. There may be occasions when the principal desires to use the security control room to make private telephone calls or to talk in private with party members or visitors. Security personnel will respect the principal's desire for privacy and depart the control room staying nearby in case summoned. A request for privacy should not be construed as an indication of a lack of confidence or trust.

2. TELEPHONES.

a. The house/hotel telephones, International Direct Dial (IDD) lines, White House lines and American Embassy lines will be operated in accordance with the printed instructions provided.

(1) House/hotel telephones. Unless directed otherwise by a key person, calls for the principal will be handled as follows:

(a) SECDEF/DEPSECDEF/CJCS: Passed directly to the principal and not routed through the control room.

(b) All other principals: Routed through the Control Room and then referred to either a key person or the principal as deemed appropriate.

(2) Embassy telephones: All calls for the principal will be routed through the Control Room and referred to a key person.

(3) IDD Telephones (OSD missions only): This telephone is a dedicated commercial line with international direct dialing capability. The number is unpublished. There are 2 extensions from the primary telephone in the security control room. These extensions are located in the principal's suite and the room of his senior military assistant. Only the telephone in the control room will ring. All calls received on this line will be referred to the party requested. There is normally an intercom switch to ring the SECDEF or his military assistant in the event the call is for them. All calls received on IDD will be logged in the control room journal. If the IDD line is inoperable, make an annotation in the control room journal and notify the MSAC immediately. Annotations of the inoperability of the IDD line must also be made on the "IDD Line Status Report" form.

(4) Secure Voice: Normally on OSD level missions, the communicators accompanying the principal will install a STU III instrument in the control room as well as in the principal's suite and the room occupied by the senior military

assistant. The STU III instrument normally is installed on the house line and the house instrument removed. Instructions for use of the STU III instrument in the unsecure mode is no different than instructions for making calls on the house line. Use the STU III to make a secure call as follows:

(a) Once both parties are on the line in the unsecure mode, insert the STU III key and turn clockwise.

(b) One of the two parties advises the other that they will "initiate".

(c) That party initiates by depressing the button marked "secure".

(d) The LED window on the telephone will display "GOING SECURE". Shortly thereafter, the agency or organization to whom you are connected with will be identified in the LED window, and the level of clearance. When this occurs, you are in the secure mode, and should be able to hear the other caller.

(e) Proceed with conversation.

(f) If the LED window displays "Secure Failed", depress the clear or unsecure button and await the return of the other party. Advise them that there is a problem and repeat the aforementioned steps. If "Secure Failed" continues to occur, either you or the other party has a problem with the phone.

(g) To terminate the call, depress the clear or unsecure button, turn the key counter-clockwise, remove the key, and hang up the receiver.

b. Security control room personnel will answer all telephones by announcing, "Title of principal", (i.e. SECDEF, CJCS, CSA, etc.) Control Room - (City), Special Agent (Name) speaking, sir."

c. All telephones in the security control room are for official use only. Their primary purpose is for communications for the principal and control of security operations. Therefore, party members other than the principal will not use the telephones in the security control room except for essential calls of short duration. In the event a dispute arises over the use of control room telephones, the matter will be referred to the MSAC and, if necessary, the principal's key person for resolution.

3. RADIO COMMUNICATIONS.

a. PSU radio net. The security control room duty agent will operate the base station for the PSU radio net established at the site of the visit. The MSAC will instruct security personnel in the operation of radio equipment.

b. Local radio nets. The security control room duty agent may be required to monitor local civilian or military police radio nets, U.S. Embassy radio nets, or the radio nets of other organizations supporting the principal's visit and to provide an interface between personnel on those nets and security forces on the PSU net.

4. DUTY JOURNAL.

a. The duty journal (CID Form 28) is a formal record of all significant activities and incidents which impact on the security force or the safety and well-being of the principal. All information pertaining to the protective services mission should be recorded at the time it occurs.

b. At a minimum, the following should be entered into the duty journal:

(1) Arrivals and departures of the principal from his place of lodging and all motorcade movements.

(2) Failure of equipment, to include telephones.

(3) Outgoing and incoming telephone calls and all messages taken for the principal or his staff.

(4) The arrival and departure of any person who enters the principal's suite. This includes guests, security agents, housekeepers, and principal's party members.

(5) Receipt of mail/packages for anyone in the party.

(6) All visitors to the area in which the principal and the official party are billeted.

(7) Baggage counts upon arrival and departure.

(8) Inventories of classified containers.

(9) Removal and return of classified material from the security control room by members of the principal's party.

(10) Disposition of classified and sensitive material waste (i.e., burn bags), to include number of bags relinquished, to whom they were relinquished, where they were relinquished, time and date.

(11) Changes of relief in the security control room.

(12) Other entries as directed by the MSAC.

5. MAIL, PACKAGES, GIFTS AND OTHER DELIVERIES.

a. Scheduled deliveries of message traffic and other expected deliveries will be made in accordance with the instructions of the MSAC. Unexpected deliveries will not be introduced onto the floor where the principal and his party are billeted until screened by the MSAC or other PSU agents. The MSAC will ensure that the hotel staff is directed to retain all deliveries at the hotel desk and to immediately notify the security control room. Upon being notified of a delivery, the duty agent will alert the MSAC, or any other PSU agent available. The notified PSU agent will screen the delivery and either direct it be delivered to the appropriate party member or coordinate with EOD or a local law enforcement agency for further screening.

b. All deliveries will be recorded in the duty journal.

c. The security control room duty agent will not leave the control room unmanned to screen deliveries.

6. ACCESS TO THE PRINCIPAL AND HIS PLACE OF LODGING.

a. Key personnel will notify the security control room duty agent of all expected visitors and instruct the agent on the action to be taken upon the arrival of the visitor. The arrival and departure of such visitors will be recorded in the duty journal.

b. Unexpected visitors requesting access to the principal will be greeted in a courteous and professional manner and their requests to visit the principal will be promptly referred to a key person. Security control room personnel will refrain from providing callers or visitors any information concerning the principal's whereabouts or his itinerary. All inquiries or requests for access to the principal will be recorded in the duty journal.

c. Security of the principal's suite is the primary responsibility of the Security Control Room duty agent. No one, except specifically designated members of the principal's official party, will be permitted unescorted access to the suite. Housekeeping personnel will be closely monitored by the Security Control Room duty agent during the entire period they have access to the suite.

d. During the periods when the principal's suite is occupied by either the principal or his wife, the hotel staff will be denied access to the suite unless requested. Room service waiters and other hotel staff who enter the principal's suite will be escorted by security personnel who will maintain visual contact with the individual(s) while in the suite.

e. All access to the principal's suite will be recorded in the duty journal.

f. The principal's suite and the Senior Military Assistant's room or Aide-de-Camp's room will be swept each morning immediately after the party departs the hotel to ensure no classified material is left unsecured.

7. CONTACT WITH THE PRINCIPAL.

a. Under normal circumstances, security personnel will not initiate direct contact with the principal. Whenever possible, communications with the principal will be made through a key person. When direct contact is necessary, it should be as brief as necessary.

b. When direct contact is initiated by the principal, security personnel will maintain a cordial, yet professional, demeanor. The MSAC will be briefed on all such incidents as soon as practical.

8. KEY CONTROL.

a. The MSAC will coordinate with the host Project Officer to preregister each member of the principal's official party. The MSAC will obtain room keys, and duplicates, for the rooms of all party members prior to the arrival of the party. This will be accomplished to expedite movement of the principal and his party into their respective rooms upon arrival at a RON location.

b. Party members will be encouraged to secure their room keys in the security control room whenever they depart the hotel. Additionally, the MSAC will attempt to obtain duplicate room keys for all rooms occupied by the official party and secure those keys in the security control room for emergency access to the rooms.

c. Upon notification that the principal is entering the hotel, the security control room duty agent will stand by with the key to the principal's suite and open the suite on a signal from the PSU agent accompanying the principal.

9. CLOSED CIRCUIT TELEVISION AND INTRUSION DETECTION SYSTEMS.

a. The MSAC will determine the requirements for closed circuit television and intrusion detections systems and supervise their installation.

b. The security control room will be the terminal and monitoring point for all surveillance and protective alarm systems. Instructions for the operation of such systems will be provided by the MSAC.

10. CONTROL AND ACCOUNTABILITY OF BAGGAGE.

a. Baggage accompanying the principal's party will be tagged and marked in a manner prescribed by the principal's administrative assistant.

b. The MSAC is responsible for the security of all baggage in transit, to include communications equipment, and will assist the administrative assistant in maintaining control and accountability. Particular emphasis will be given to the expeditious handling and delivery of the principal's personal baggage and the classified material. The principal's personal baggage will normally be transported in the trunk of his vehicle and/or the trunk of the chase vehicle.

c. Communications personnel will accompany their equipment during all movements and will be responsible for its accountability.

d. Security personnel assigned to the baggage detail will ensure that all baggage remains under strict control of security forces and will complete a baggage accountability report. All porters handling baggage will be accompanied by security/communications personnel at all times. No items of baggage will ever be left unattended by security/communications personnel.

e. Baggage arriving at an overnight site without the proper tag or markings will NOT be delivered to the floor where the party is billeted until positively identified.

f. Gratuities or porter fees will be reimbursed by the trip coordinator or Aide-de-Camp to the principal or charged to the security control room in the case of DoD missions.

g. In preparation for departure from overnight sites, a baggage pickup point will be designated by the MSAC. Each individual in the principal's party will be notified of the pickup point and will be responsible for ensuring his/her baggage is delivered to the pickup point by the designated time. Baggage notices will be posted as deemed appropriate (i.e., size of party).

h. At the pickup point, the MSAC will ensure all baggage is properly tagged and inventoried.

i. Again, security personnel of the baggage detail will ensure strict control of each item of baggage until it is delivered to its next location or loaded aboard the aircraft.

j. When baggage is moved in the motorcade, the MSAC will ensure that vehicles are not released until all baggage is unloaded and accounted for.

11. CONTROL AND ACCOUNTABILITY OF CLASSIFIED MATERIAL.

a. All classified material will be off-loaded from the aircraft and moved to the security control room under the supervision of a special agent. At the time the classified material is off-loaded from the plane and loaded in a vehicle(s) or van(s), a count will be conducted by the special agent escorting the classified

material and this count will be verified in writing by another security agent, military policeman, or communicator. When classified material arrives at the hotel, the special agent will accompany the classified material to the security control room.

b. Once all classified material is in the security control room, a count will be conducted by the control room duty agent and the special agent that escorted the classified material. This count will be logged into the control room journal and a classified container report will be completed.

c. Access to the classified material will be granted to members of the official party. If any classified material is removed from the control room, it will be logged in the control room journal.

d. The same procedures will be utilized when removing the classified material to be transported to the aircraft upon departure.

e. A count of the classified material will be done when control room agents change shifts and the count will be logged in the control room journal.

f. AT ALL TIMES CLASSIFIED MATERIAL WILL BE UNDER THE DIRECT CONTROL OF AN AMERICAN WITH AN APPROPRIATE SECURITY CLEARANCE.

12. SPECIAL PROCEDURES FOR SECDEF/DEPSECDEF BAGGAGE/CLASSIFIED HANDLING.

a. Personal baggage, classified material containers, and sensitive material/equipment containers (i.e. physician's medical equipment and protocol gift containers), required to be stowed topside on the aircraft are coded as such by having a piece of red yarn affixed to the container.

b. Classified material containers and sensitive material/equipment containers coded with red yarn are also marked "Control Room" on the baggage tag.

c. All personal baggage, whether topside or in the cargo hold (belly) of the aircraft, and other equipment containers stowed in the belly, are clearly marked with either the individual's room number or "Control Room" on the baggage tag.

d. Normally items topside are off-loaded before those in the belly.

e. During the off-loading process of items topside, personal baggage (i.e. suit bags, handbags, etc., which reflect a room number on the bag tag), should be placed to the side and not loaded into the vehicle designated to transport the classified and sensitive material containers. After the classified transport vehicle is loaded and secured, the personal baggage can be loaded onto the same truck

used to transport the item s off-loaded from the belly. This simplifies both the delivery and accountability process.

f. Once the baggage convoy arrives at the hotel, the items in the classified transport vehicle should be delivered to the security control room before personal baggage is delivered to individual rooms.

g. If party member rooms are scattered throughout different wings on a floor or are on different floors, it is sometimes simpler and more efficient to first deliver all personal baggage to a centralized location near the security control room. At that point it can be more easily segregated and then delivered to the various rooms. This is particularly true if the quantity of personal bags exceeds 60 bags.

h. For departures, the following procedures should be followed to simplify the accountability and delivery process.

(1) For party members occupying rooms on floors different from that of the security control room, baggage notices should be modified to reflect that their baggage should be delivered to the security control room at the designated time.

(2) All personal baggage bearing red yarn should be loaded onto the same vehicle with the classified/sensitive material containers so that it doesn't become confused with baggage and equipment destined for the belly.

13. DISPOSITION OF CLASSIFIED/SENSITIVE MATERIAL WASTE.

a. During the advance phase of the mission, the MSAC will have identified, by name, the appropriate U.S. Embassy or action officer representative to whom classified and/or sensitive waste will be relinquished for disposal.

b. During the operational pre-brief, the MSAC will assign one agent the responsibility for disposing of the burn bags. The MSAC will also explain the mechanism for disposition (i.e. either the representative comes to the security control room t o take custody of the burn bags from that agent or that agent will personally deliver the burn bags to the representative at either the Embassy control room or the Embassy itself).

c. During the execution phase of the mission, burn bags will be maintained in the security control room for disposal of classified and/or sensitive material waste.

d. Once a burn bag is full, it will be properly sealed (taped and stapled shut), by the duty agent.

e. During clean-up operations, following wheels-up, the designated agent will properly dispose of all burn bags in accordance with the instructions from the MSAC during the pre-brief.

f. The control room duty journal will then be annotated with the information required in paragraph 4b, this SOP.

g. During the post mission critique, the MSAC will personally verify that the foregoing actions concerning disposition were accomplished.

14. BOMB THREATS.

a. Because of the increase in the frequency and seriousness of terrorist bombing, it is important that all protective service operations have an effective bomb plan. This plan will establish what actions are to be taken when a bomb threat is received and who is responsible for what, where and how. When a threat is received, there are a number of considerations which should be taken into account. The person receiving the threats by telephone should attempt to elicit as much information as possible from the caller and should fill out a bomb threat checklist.

b. The military police or police force having jurisdiction should be notified immediately. Other notifications to agencies such as the explosive ordnance detachment (EOD), fire department, ambulance and facilities engineers should also be made as appropriate to the area and existing regulations.

c. A decision whether or not to evacuate the premises must be made. This is a very difficult decision which must be based on an evaluation of all circumstances. Some considerations are:

(1) An evaluation of the person/group making the threat to include motivation and demeanor. This may indicate whether the threat is bonafide or a hoax.

(2) When and where the bomb is set to go off.

(3) Whether the premises have been properly searched by persons occupying them.

(4) Type of building structure and how prone it is to damage.

(5) Where regulations are in existence, they take precedence.

d. Whether evacuation is directed or not, a search must be conducted. Some points to keep in mind are:

(1) The search must be systematic, planned, orderly and complete.

(2) If you know the location of the bomb start there. HOWEVER, DO NOT TOUCH SOMETHING YOU THINK MIGHT BE THE BOMB.

(3) The search party should include individuals familiar with the building or area if possible; and, should be conducted with EOD personnel.

(4) Searchers should assume that any suspected explosive device or package is dangerous and deadly. They should not touch, move or disturb the object since it may contain an anti-disturbance device. THE SUSPECTED DEVICE SHOULD ONLY BE HANDLED BY QUALIFIED EOD PERSONNEL.

15. IT SHOULD BE EMPHASIZED THAT BASED UPON THE VERY NATURE OF ANY PROTECTIVE SERVICE MISSION, THIS SOP CANNOT BE CONSIDERED ALL INCLUSIVE. COMMON SENSE AND SOUND JUDGMENT MUST BE UTILIZED AT ALL TIMES BY ALL MEMBERS OF THE PROTECTIVE SERVICES DET AIL TO EN-SURE THE SUCCESSFUL ACCOMPLISHMENT OF THE MISSION.

PROTECTIVE SERVICES
SECURITY CONTROL ROOM STANDING OPERATING PROCEDURES

I certify that I have read and understand the policies and procedures set forth in this SOP:

PRINTED NAME SIGNATURE DATE

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

8 Encls MISSION SAC

1. Bomb Threat Checklist
2. Duty Roster
3. Room Assignments
4. Itinerary
5. Motorcade/Helo Assignments
6. Telephone Contact Sheet
7. Principal's Protocol Bio
8. Principal's Medical Bio (PSO only)

Appendix O
Preparation of FD Form 249 (FBI Criminal History Fingerprint Card) and FBI/DOJ Form R-84 (Final Disposition Report).

O-1. General.

This appendix provides detailed instructions for the preparation of FD Form 249 and FBI/DOJ Form R-84 and lists those offenses, which require the submission of criminal history records to the FBI. (See Figure 1)

O-2. Offenses.

The following is a list of offenses under the UCMJ that (together with the initiation of military judicial action or the imposition of non-judicial punishment) requires the forwarding of FD Form 249 to the FBI.

Article	Specific Offense
78	Accessory after the fact for crimes listed in this appendix
80	Attempts to commit crimes listed in this appendix
81	Conspiracy to commit crimes listed in this appendix
82	Solicitation
85	Desertion
90	Assaulting a superior officer
91	Striking or assaulting warrant, noncommissioned, or petty officer
94	Mutiny or sedition
95	Resistance, breach of arrest, and escape
106	Spies
106a	Espionage
107	False official statements (in conjunction with another crime investigated by the (USACIDC)

108	Military property, selling, or otherwise wrongfully disposing of Military property, willfully damaging, destroying, losing, or suffering to be lost, damaged, destroyed, sold, or Wrongfully disposed of; of a value of more than $100, or any firearm, explosive, or incendiary device
109	Willfully destroying or damaging private property
111	Drunk driving
112a	Wrongful use, possession, etc., of controlled substances
116	Riot
118	Murder
119	Manslaughter
120	Rape, carnal knowledge
121	Larceny and wrongful appropriation
122	Robbery
123	Forgery
123a	Bad checks of a value of more than $100
124	Maiming
125	Sodomy
126	Arson
127	Extortion
128	Assault
129	Burglary
130	Housebreaking
131	Perjury

132	Frauds against the United States
134	Assault, indecent
	Assault with intent to commit murder, voluntary manslaughter, rape, robbery, sodomy, arson, burglary, or housebreaking
	Assaulting a federal officer in performance of duties
	Bribery and graft
	Burning with intent to defraud
	False pretenses, obtaining services under, of a value of more than $100
	False swearing
	Firearm, discharging wrongfully as to endanger human life
	Fleeing the scene of an accident
	Homicide, negligent
	False impersonation with intent to defraud
	Indecent acts or liberties with a child
	Indecent language communicated to a child under the age of 16 years
	Indecent acts with another
	Kidnapping
	Mails, taking opening, secreting, destroying, or stealing
	Mails, depositing or causing to be deposited obscene matters in
	Misprision of serious offense
	Obstructing justice

	Pandering and prostitution
	Perjury, subornation of
	Public record, altering, concealing, removing, mutilating, obliterating, or destroying
	Seizure, destruction, removal, or disposal of property to prevent
	Soliciting another to commit an offense, for crimes listed in this Appendix
	Stolen property, knowingly receiving, buying, or concealing, of a value of more than $100
	Testify, wrongful refusal
	Bomb threat or hoax
	Threat, communicating
	Weapon, concealed or carrying
	Offenses under the Federal Assimilative Crimes Act (18 U.S.C., reference (h)), charged as a violation of Article 134, UCMJ, which has a maximum punishment of more than one year

O-3. Instructions for completing FD Form 249

a. All narrative entries will be typed, if possible. If printed, they will be printed in black or blue-black ink. Broad, felt-tipped pens should not be used.

b. Fingerprints must be rolled carefully and smoothly to avoid smudging or making unclassifiable prints. Specific techniques for taking fingerprints are contained in FM 19-20.

c. Fingerprints determined by the FBI to be unclassifiable will be returned to the preparing office through the Crime Records Center for reprinting.

d. The following specific instructions are keyed to the numbered blocks on the FD Form 249. Data fields preceded by an asterisk (*) must be completed in order for your fingerprint card to be processed by the FBI. However, all data fields are important and should be completed if the information is known.

(1) Name (NAM) Block: Enter the name obtained from the subject in this field. The format is last name followed by a comma (,) first and middle name, if any. Suffix denoting seniority (Jr., Sr., II etc.,) should follow the middle or first name.

(2) Signature of Person Fingerprinted Block: Obtain signature of the person fingerprinted, in ink.

(3) Social Security Number (SOC) Block: List subject's social Security number if known. Additional Social Security numbers used by the subject may be entered in the "Additional Information/Basis for Caution" Block on back of the fingerprint card.

(4) Alias/Maiden Name Bock: List other names used by the subject that are different than the name entered in the NAM block. Also, list the signature name as an AKA if different than the name that appears in "NAM" block. If more space is needed, enter additional aliases in the "Additional Information/Basis for Caution" block on face side of the fingerprint card. Maiden names and all previous married names of females should be entered in the alias field, if known.

(5) FBI Number (FBI) Block: Enter the assigned FBI number for subject, if known.

(6). State Identification Number (SID) Block: Leave blank.

(7) *Date of Birth (DOB) Block: Enter DOB in month, day and year format. If a complete DOB is not known, enter approximate age.

Note: Fingerprint cards of persons 99 years old or older are not processed by the FBI.

List additional dates of birth on face side of fingerprint card in the "Additional Information/Basis for Caution" block.

Note: If the DOB block is left blank, and the card does not have a FBI number quoted, the card will be returned without processing.

(8) Sex (SEX) Block: Sex must be indicated by either "F" (female) or "M" (male).

Note: Indicate in the "Additional Information/Basis for Caution" block is the subject is a transvestite or has undergone a sex change operation. If applicable, list any opposite gender names used in the "Alias" block.

(9) Race (RAC) Block: Race must be indicated by one of the following one-character alphabetic characters: A=Asian, B=Black, I=American Indian, W=White

ADDITIONAL EXPLANATIONS OF RACE CATEGORIES		
A	-	Indicates Pacific Islander, Chinese, Japanese, Polynesian, Korean, and Vietnamese
B	-	Includes Negro, "N," and Colored
I	-	Includes Alaskan native, Eskimo, and American Indian
W	-	Includes Caucasian, Mexican, Latin, Puerto Rican, Cuban, Central/South American, and other Spanish culture or origin, regardless of race

(10) Height (HGT) Block (3 characters): Height must be expressed in feet and inches. should be rounded off to the nearest fractions of an inch.

(11). Weight (WGT) Block (3 characters): Weight must be expressed in pounds. Fractions of a pound should be rounded off to the nearest pound.

(12) Eye Color (EYE) Block (3 characters): Indicate eye color by one of the following three-character codes:

If description is:	List data in block as:
BLACK	BLK
BLUE	BLU
BROWN	BRO
BROWN	BLU
GRAY	GRY
GREEN	GRN
HAZEL	HAZ
MAROON	MAR
PINK	PNK
UNKNOWN	XXX

(13) Hair Color (HAIR) Block (3 characters): Indicate hair color by one of the following three-character codes:

If description is:	List data in block as:
BALD	BAL
BLACK	BLK
BLOND	BLN
BROWN	BRO
GRAY	GRY
RED	RED
SANDY	SDY
WHITE	WHI
UNKNOWN	XXX

(14) Fingerprint Impression Blocks (Individual & Simultaneous) It is very important that care be taken to roll the fingers from nail to nail when taking the individual finger impressions. This will help ensure legibility. Roll the prints in the correct sequence. Note the right and left-hand designations in the finger blocks, obtain simultaneous "plain" impressions and indicate amputated finger(s) or finger(s) missing at birth.

Note: Fingerprint cards received with contributor and/or state bureau markings will be rejected (i.e., ident symbols, cross marks, or finger impression already classified).

(15) Juvenile Fingerprint Block: Juvenile fingerprint cards will be "retained" provided the card contains criterion charges and there is no indication that the card should be returned to your agency.

(16) Date of Arrest (DOA) Block: Enter the date the subject was arrested in month, day and year format. If contributor is a prison/jail, enter the date received.

(17) *Originating Agency Identifier (ORI) Number Block: Only the ORI of the Crime Records Center will be listed in this block. The correct ORI for the Crime Records Center is as follows:

VAUSA1400
US ARMY
Ft Belvoir, VA

To order fingerprint cards or other related forms, contact the FBI at (202) 324-5262, or submit Form 1-178 to:

Federal Bureau of Investigation
J. Edgar Hoover Building
Personnel Division, Printing Unit, Room 1B973
935 Pennsylvania Ave., NW.
Wash, DC 20535-0001

Note: You should never borrow preprinted fingerprint cards from another agency or load your agency's preprinted fingerprint cards to another agency. Ensure that your cards are requested with the "VAUSA1400" ORI. Further, If a reply is desired check the "YES" block. A reply will be sent only if the "YES" block is checked.

(18) Send Copy to (SCT) Block:

(19) Date of Offense (DOO) Block: Enter date offense was committed, if known.

(20) Place of Birth (POB) Block (state or country): List the state, territorial possession, province (Canadian) or country of birth. Use the correct abbreviation for foreign countries or correctly spell the name of the country. Do not list county as a POB.

(21) Country of Citizenship: If born in the United States, list as "U.S.," otherwise, list country.

(22) Miscellaneous Number (MNU) Block: The MNU is an identifying number associated with the subject such as U.S. Military Service Number, passport number, etc. Enter MNU and indicate description according to the following chart.

DESCRIPTION

- Air Force Serial Number
- Alien Registration Number
- Army Serial Number/National Guard Serial number/Air National Guard Serial Number, and U.S. Cost Guard Serial Number
- Bureau Fugitive Index number
- Canadian Social Insurance Number
- Mariner's Document or Identification Number
- Marine Corps Serial Number
- Royal Canadian Mounted Police Identification Number (FPS Number)
- National Agency Case Number-Military*
- Navy Serial Number
- Identification Order Number
- Passport Number
- Port Security Card Number
- Selective Service Number
- Veterans Administration Claim Number

(23) Scars, Marks, Tattoos, (SMT) and Amputations Block
List SMT and/or amputations.

(24) Residence/Complete Address
Enter complete residential address obtained from subject's identification.

(25) Official Taking Fingerprints: Enter name or number of Official taking fingerprints.

(26) Local Identification/Reference Number Block: Enter the ROI number for which the individual is listed as the subject, deleting the letters "CID". For example an investigation conducted by the Fort Sam Houston Resident Agency in 1994 would be entered as 9404412345. As this is a ten-character field, do not include the local sequence number. Under no circumstances should a sequence only action fingerprint card be submitted to the FBI.

(27) Photo and Palm Prints Block Indicate if photo and/or palm prints are available.

(28) Employer Block: Enter U.S. Army. If U.S. Government, indicate agency, if military, list branch of service and serial number. Otherwise, indicate company or agency where subject is employed.

(29) Occupation Block: Indicate occupation, if available. Enter the title of the subjects primary MOS.

(30) *Charge/Citation Block: Enter each offense for which the individual is listed as a subject, beginning with the most serious offense, using the narrative of the UCMJ offense (i.e., Murder, Rape, Assault). Continue in block 48 on the reverse side, if necessary.

Note: Only those offenses listed in paragraph 0-2 above will be reported to the FBI.

(31) Disposition Block: Final disposition and date: Enter the specific finding (e.g., guilty, not guilty, dismissed, etc.) and the disposition, as approved by the convening authority, for each offense listed in Charge/Citation block in the adjacent Disposition Block. If an offense titled is tried as a lesser or different offense, so indicate. For example, if the first offense for which the individual was listed as the subject was robbery, and the accused was found guilty of the lesser included offense.

EXAMPLES
Guilty of Murder, Article 118, Life sentence, BCD, Total Forfeiture, 1 Apr 98.
Guilty of Larceny, Article 121, 2 yrs CHL, BDC, Total Forfeiture, 1 Apr 98

Under no circumstances will non-judicial punishment under Article 15 of the UCMJ be listed as a guilty finding. The disposition of "conviction" or "guilty" will only be reported for crimes prosecuted at trials by general, special, or summary court-martial yielding a plea or finding of guilty. Adverse findings stemming for non-judicial punishment under Article 15 of the UCMJ should be listed as follows:

Received non-judicial punishment under Article 15, UCMJ, reduced from E-5 to E-3, forfeited $500.00 for 2 months, and received 45 days extra duty.

As a reminder, in addition to judicial findings, the DOD requirement for submission fingerprint to the FBI is non-judicial punishment imposed by an officer in the grade of Major or Lieutenant Commander under Article 15 of the UCMJ (Field Grade Article 15), or the approval of a request for discharge, retirement, or resignation in lieu of court-marital.

(32) Additional Block (Charges): Enter charges when more than three and number each.

(33) Additional Block (Dispositions): Enter dispositional data when more than three and number each.

(34) Additional Information/Basis for Caution Block: Enter additional or multi-informational data that did not fit in blocks provided, such as: additional DOB, additional names, etc. In addition, this block also provides reason for caution. State information which indicates a condition which could be expected to continue (e.g., escape risk, armed and dangerous, martial arts, etc.).

(35) State Bureau Stamp Block: When card is a single source state participant, and your card does not reflect your state bureau identification stamp, the card will be immediately returned to the state bureau/submitting agency.

Note: At this point a quality review of arrest and personal descriptor data is extremely important. This step can improve the quality of the cards submitted and help eliminate immediate rejects (i.e., cards returned by the FBI without processing).

0-4 Instructions for completing FBI/DOJ Form R-84

a. The FBI/DOJ Form R-84 will be completed (Except for final disposition information) at the same time as the FD Form 249. This will avoid having to relocate and arrange for the presence of the subject a second time after final disposition is known.

b. The following instructions are keyed t the numbered blocks on the FBI/DOJ Form R-84 shown at figure 2 of this appendix.

(1) FBI number: Enter the number assigned to the subject by the FBI, if known.

(2) Name of Fingerprint Card submitted to the FBI: Enter exactly as entered in block 1 of DF Form 249.

(3) Date of Birth: Enter the same manner as in block 7 of FD 249.

(4) Henry Fingerprint Classification: Enter the classification assigned by the FBI, if known.

(5) State Bureau Number: Leave blank.

(6) Social Security Number: Self-explanatory.

(7) Contributor of Fingerprints: Enter as follows:

VAUSA1400
US ARMY
Ft Belvoir, VA

(8) Arrest Number (OCA): Enter the CID report of investigation number as in block 26 of FD Form 249.

(9) Date arrested or received: Enter the date that fingerprints are taken. This will be the same as block 16 of FD Form 249.

(10) Offense charged at the time of arrest: Enter the same information as in block 30 of FD Form 249.

(11) Final disposition and date: Enter the specific finding (e.g., guilty, not guilty, dismissed, etc.) and the disposition, as approved by the convening authority, for each offense listed in block 10. Disposition information should be numbered in the same sequence as in block 10; thus it is not necessary to repeat the charges here. If an offense titled is tried as a lesser or different offense, so indicate. For example, if the first offense for which the individual was listed as the subject was robbery, and the accused was found guilty of the lesser included offense of larceny, the entry would appear as:

Guilty of larceny, Art 121, UCMJ: 2 yrs CHL, BCD, Total forfeiture. 1 Apr 93.

(12) Form submitted by: Enter the name and organization (with ORI designator) of the CID unit submitting the Final Disposition Report.

(13) Court ordered expungement: Leave blank.

O-5 Reorder of Forms FD 249 and R-84.

The forms FD-249 and R-84 should be reordered directly from the FBI using reorder forms provided by the FBI or by letter addressed to the Federal Bureau of Investigation, J. Edgar Hoover Building, Personnel Division, Printing Unit, Room 1B973, 935 Pennsylvania Ave., NW. Washington, DC 20535-0001. When requesting forms from the FBI, it is essential that they be advised to preprint the contributor as VAUSA1400, U.S. Army Crime Records Center, 6010 6th Street, Ft Belvoir, VA 22060-5585. The ORI number and address of the requesting office must be given as the shipping address.

Appendix P
Daytime Practical Pistol Qualification Course

P-1. General

a. The course of fire in paragraph P-2 below is conducted from the closest to the longest ranges to allow shooters maximum feedback while shooting.

b. Shooters will be allowed to briefly inspect their targets between stages of fire.

c. Because of the short ranges involved, the time limits imposed are essential for the qualification process to be meaningful. If shooters are allowed extra time and alibis, their abilities to handle their weapons in law enforcement/combat situations will not be accurately measured and those requiring additional training and practice will not be identified.

d. All rounds not fired within the time limit specified for each station will be counted as misses. If a shooter fires any rounds after the command cease fire or other signal used, 5 points will be subtracted from the shooter s score for each round fired after the signal. For practical purposes, a two second lag should be allowed after the signal before this rule is imposed.

e. Ensure compliance with safety requirements as outlined in appendix R of this regulation, AR 385-63, FM 23-9 and FM 23-35.

f. Shooters are authorized 12 rounds for practice fire in addition to the 60 rounds required for qualification.

P-2. Description of course

a. Station 1

(1) Distance: 3 meters

(2) Number of Rounds: 12 rounds

(3) Position: Modified Isosceles

(4) Procedure: Shooters load one 6 round magazine, decock the weapon, and reholster the weapon. A total of 15 seconds will be allotted for shooters to draw the weapon, assume the position, and engage the target with 12 rounds. On the command, shooters will engage the target with 6, rounds, emergency reload, and fire the remaining 6 rounds.

Ready right? Ready left? The firing line is ready Shooters ready position, commence firing

Logistics, two 6 round magazines

b. Station 2

(1) Distance: 5 meters

(2) Number of rounds: 12 rounds

(3) Position: Modified Point Shoulder

(4) Procedure: Shooters load one 6 round magazine, decock, and reholster the weapon. A total of 15 seconds will be allotted for shooters to draw the weapon, assume a modified point shoulder position, and engage the target with 12 rounds. On the command, shooters will engage the target with 6 rounds, emergency reload, and fire the remaining 6 rounds.

Ready right? Ready left? The firing line is ready Shooters ready position, commence firing

Logistics, two 6 round magazines

c. Station 3

(1) Distance: 7 meters

(2) Number of Rounds: 12 rounds

(3) Position: High cover

(4) Procedure: Shooters load one 12 round magazine, decock the weapon, and assume a high cover position. On the command, shooters will have 3 seconds to bring the weapon to a firing position, engage the target with 2 rounds, and then return to the high cover position. This 3 second drill will be continued until all 12 rounds have been fired.

Ready right? Ready left? The firing line is ready Shooters ready position, commence firing

Logistics, on 12 round magazine

d. Station 4

(1) Distance: 15 meters

(2) Number of Rounds: 18 rounds

(3) Position: Kneeling Barricade Supported

(4) Procedure: Shooters load one 6 round magazine, decock and reholster. On the command, shooters will assume a strong hand kneeling barricade position, draw the weapon, and engage the target 6 rounds. Shooters will then emergency reload, assume an over barricade position, and engage the target with 6 rounds.

Continuing, shooters will then emergency reload, assume a weak hand kneeling barricade position, and fire the remaining 6 rounds. A total of 90 seconds will be allotted to fire all 18 rounds.

Ready right? Ready left? The firing line is ready Shooters ready position, commence firing

Logistics, three 6 round magazines

e. Station 5

(1) Distance: 25 meters

(2) Number of Rounds: 6 rounds

(3) Position: Standing Barricade Supported

(4) Procedure: Shooters load one 6 round magazine, decock, and reholster the weapon. On the command, shooters will have 25 seconds to draw the weapon, assume a standing strong hand supported barricade position, and engage the target with 6 rounds.

Ready right? Ready left? The firing line is ready Shooters ready position, commence firing

Logistics, one 6 round magazine

f. Station 6 **This station is not part of record qualification, familiarization

ONLY

(1) Distance: 7 Meters

(2) Number of rounds: 12 hollow-point rounds

(3) Position: Modified Point Shoulder

(4) Procedure: Shooters load one 6 round magazine, decock, and reholster the weapon. A total of 15 seconds will be allotted for shooters to draw the weapon, assume a modified point shoulder position, and engage the target with 12 rounds. On the command shooters will engage the target with 6 rounds, emergency reload and fire the remaining 6 rounds.

Ready right? Ready Left? The firing line is ready Shooters ready position, commence firing.

Logistics, two 6 round magazines

Course Logistics

Total magazines needed: 11

8 magazines with 6 rounds of ball ammunition

1 magazine with 12 rounds of ball ammunition

2 magazines with 6 rounds of hollow-point ammunition

Total rounds of ball ammunition: 60

Total rounds of hollow-point ammunition: 12

Total rounds: 72

One type “S” silhouette target per shooter.

* NOTES:

EMERGENCY RELOAD: Is the term used when you have fired all the rounds in the weapon and the slide is locked to the rear.

COMBAT RELOAD: Is accomplished by dropping the magazine from the weapon while a round is still in the chamber.

READY POSITION: The shooter has a two-handed grip, elbows bent, and the forearms are parallel to the ground.

HIGH COVER: The shooter has a two-handed grip, both arms are extended into a shooting position, but the muzzle is lowered pointed below the belt-line of suspect.

MODIFIED ISOSCELES: The shooter's feet and shoulders are parallel to the target, shoulders over balls of the feet. Weight is equally distributed on both feet, feet should be shoulder width apart or more, knees slightly bent. Both arms are extended to ward the target, forming a triangle. Vision is best with head erect (see figure P-1).

MODIFIED POINT SHOULDER: The shooter's body is upright and the strong side foot and shoulder are moved to the rear so that they are approximately 45 degrees to the target. The feet are spread shoulder width apart with the body weight equally distributed. The knees may be slightly bent. The weapon is drawn, pointed toward target, both elbows bent and pointed downward, with the strong arm in a pushing motion, and the support arm bent in a slight pulling motion. This push-pull effect on the weapon creates an isometric tension which reduces recoil and lessens recovery time. Vision is best with head erect (see figure P-2).

Appendix Q
Nighttime Practical Pistol Sustainment Course

Q-1 General

a. The M11 pistol is equipped with tritium night sights; therefore, shooters must be properly trained and have confidence in the sight system.

b. The course of fire in paragraph Q-2 must be conducted in a low light environment. All reloading should be completed without visual aid; therefore, shooters should be discouraged from looking at the weapon during reload.

c. Special safety precautions must be taken due to the low light environment. All weapons should be cleared and holstered before moving to the next station.

d. Shooters are authorized 12 rounds for night instructional fire and 24 rounds for night practice fire, in addition to the 24 rounds required for the night sustainment fire.

Q-2. Description of Course

a. Station 1

(1) Distance: 5 meters

(2) Number of Rounds: 6 rounds

(3) Position: Modified Point Shoulder

(4) Procedure: Shooters load one 6 round magazine, decock, and reholster the weapon. On the command, shooters will have 20 seconds to draw the weapon, assume a modified point shoulder position, and engage the target with 6 rounds. Upon completion, remove your magazine, leave the slide locked to the rear and standby for a range safety NCO to clear your weapon. At the range safety NCOs direction, let the slide go forward, decock and reholster.

Ready right? Ready left? The firing line is ready Shooters ready position, commence firing

Logistics, one 6 round magazine

b. Station 2

(1) Distance: 5 meters

(2) Number of Rounds: 12 rounds

(3) Position: Modified Point Shoulder

(4) Procedure: Shooters load one 6 round magazine, decock, and reholster the weapon. A total of 30 seconds is allotted to draw the weapon, assume a modified point shoulder position, and engage the target with 12 rounds. On the command, shooters will engage the target with 6 rounds, emergency reload, and fire the remaining 6 rounds. Upon completion, remove your magazine, leave the slide locked to the rear and standby for a range safety NCO to clear your weapon. At the range safety NCOs direction, let the slide go forward, decock and reholster.

Ready right? Ready left? The firing line is ready Shooters ready position, commence firing

Logistics, two 6 round magazines

c. Station 3

(1) Distance: 15 meters

(2) Number of Rounds: 6 rounds

(3) Position: Modified Point Shoulder

(4) Procedure: Shooters load one 6 round magazine, decock, and reholster the weapon. On the command, shooters will have 20 seconds to draw the weapon, assume a modified point shoulder position, and engage the target with 6 rounds. Upon completion, remove your magazine, leave the slide locked to the rear and standby for a range safety NCO to clear your weapon. At the range safety NCOs direction, let the slide go forward, decock and reholster.

Ready right? Ready left? The firing line is ready Shooters ready position, commence firing

Logistics, one 6 round magazine

Course Logistics

Total magazines needed: 4

4 magazines with 6 rounds

Total rounds: 24

One type S silhouette target per shooter

* NOTES

EMERGENCY RELOAD: Is the term used when you have fired all the rounds in the weapon and the slide is locked to the rear.

COMBAT RELOAD: Is accomplished by dropping the magazine from the weapon while a round is still in the chamber.

READY POSITION: The shooter has a two-handed grip, elbows bent, and the forearms are parallel to the ground.

HIGH COVER: The shooter has a two-handed grip, both arms are extended into a shooting position, but the muzzle is lowered pointed below the belt line of suspect.

MODIFIED ISOSCELES: The shooter's feet and shoulders are parallel to the target, shoulders over balls of the feet. Weight is equally distributed on both feet, feet should be shoulder width apart or more, knees slightly bent. Both arms are extended to ward the target, forming a triangle. Vision is best with head erect (see figure P-1).

MODIFIED POINT SHOULDER: The shooter's body is upright and the strong side foot and shoulder are moved to the rear so that they are approximately 45 degrees to the target. The feet are spread shoulder width apart with the body weight equally distributed. The knees may be slightly bent. The weapon is drawn, pointed toward target, both elbows bent and pointed downward, with the strong arm in a pushing motion, and the support arm bent in a slight pulling motion. This push-pull effect on the weapon creates an isometric tension which reduces recoil and lessens recovery time. Vision is best with head erect (see figure P-2).

Appendix R
Range Operations and Safety

R-1. Range facilities

a. Range facilities and availability will vary considerably from location to location. It is incumbent upon each commander/SAC to locate suitable facilities for marksmanship training and qualification that will be available for use within the area of responsibility. If subordinate units are in close proximity to the parent organization, the training and qualification firing may be consolidated for better control and utilization of resources. Indoor or outdoor ranges may be used depending on availability, with the only requirement being that the range can support the maximum distance (25 meters) required. If military ranges are not available, the local rod and gun club or our civilian law enforcement counterparts may have range facilities which are suitable and could be used for necessary firing.

b. The fabrication and type of barricades required in the course is contingent upon local facilities available for use. Some installations will build and store barricades for continued use and some will not, hence local coordination is essential well in advance of any scheduled firing. No specific standards have been prescribed on what type of barricades should be used to allow ample opportunity for local initiative. Barricade could be readily adapted from such locally available material s as 55 gallon drums, wooden pallets, shipping crates, used doors, sandbag walls, vehicle doors, vehicle fenders, or garbage cans. Varying and changing types of barricades being used can add to creating a more realistic shooting situation that an agent may encounter in a real situation. The purpose is to encourage the agent to seek protective cover that is readily available at the scene and to present the smallest target possible for the enemy to engage.

R-2. Medical support

a. Most large range areas normally have a central medical support facility, i.e., a first aid station with an ambulance and driver. The first aid station normally has telephone contact with all ranges. If this type support is available, it will be used when conducting firing. Special arrangements may have to be made for nighttime firing.

b. As a minimum, a first aid kit will be available and radio contact will be maintained with the local military police or any facility or organization that can immediately react and provide emergency care if required to do so.

R-3. Ammunition.

Training ammunition utilized at ranges for qualification and sustainment is authorized by HQUSACIDC for each unit based upon the requirements in DA Pam 350-38, tables 5-31 and 5-37.

R-4. Safety

a. The strictest discipline must be maintained at all times on the range in order to prevent accidents and injuries. Range safety rules can be found in AR 385-63, FM 23-9, FM 23-35, and local range regulations. Some of the main points to remember are as follows:

(1) Treat all firearms as though they were loaded.

(2) Always point the muzzle of the weapon in a safe direction.

(3) Keep your finger outside the trigger guard until you are on target and ready to fire.

(4) Be sure of your target and what is beyond it.

b. The commander of using units will:

(1) Ensure that all personnel are familiar with local range procedures and safety requirements.

(2) Designate an officer-in-charge (OIC), who can be a commissioned officer, warrant officer (WO), or noncommissioned officer (NCO) for the range to be responsible for the safe conduct of firing and proper use of facilities.

(3) Comply with installation procedures for certifying individuals who will perform the duties of OIC, WOIC, NCOIC, or range safety officer (RSO) to ensure they are:

(a) Competent and properly instructed in the performance of their duties.

(b) Knowledgeable of the weapons systems for which they are responsible.

(4) Coordinate plans for firing exercises and maneuvers with range control.

c. The officer in charge will:

(1) Be responsible for the overall safe conduct of training and proper use of facilities.

(2) Be present at the unit firing area.

(3) Appoint a RSO when required to help perform safety responsibilities. Additional assistant range safety officers (ARSO) may be appointed as needed. The need for a RSO will depend on the complexity of the exercise, number of participants, type of weapon, and physical separation of OIC from firing point. When nuclear, biological, chemical (NBC) training is being conducted, the OIC and RSO must be NBC qualified.

(4) Determine when it is safe to fire.

(5) Supervise the procedures for misfires, hang-fires, and cook-offs.

(6) Ensure required communications are established and maintained.

d. The range safety officer will:

(1) Be responsible for the final determination before firing that:

(a) Weapons are properly positioned.

(b) Only authorized ammunition is used.

(c) Weapons are within prescribed safety limits and verified.

(d) Appropriate safety measures are taken and the surface danger zone is clear of personnel. (This includes closing of barriers denying entry into the impact area and the posting of road guards.)

(e) Proper hearing protection is worn by personnel engaged in firing.

(2) Order an immediate cease fire or check fire when any unsafe condition is observed.

(3) On completion of firing, verify weapons are clear to the OIC and range control and record duds and their approximate location.

Appendix S
Internal and External Sources

Generally, information sought by an investigator can be thought of as coming from either internal or external sources. The best place to start the search for information is internally. Law enforcement/investigative records and reports are the most readily available and therefore cause the least problems or frustrations. Law enforcement/investigative agencies have most, if not all, of the following reports and records:

Internal Sources
Types of Information

Incident or offense reports:
Name, address, telephone numbers, statement of facts (who, what, where, when, why, how)

Arrest records:
Name, address, telephone numbers, DOB, physical description, Social Security no., fingerprints, offenses charged

Traffic citations (reports):
Name, address, DOB, driver's license number, auto registration number, infraction location, signature

Traffic accident reports:
Name, address, driver's license number and state, auto registration number, vehicle ID number, location of accident, time of accident, names of others in vehicle

Name index files:
Name, address, telephone numbers, aliases, associates, relatives, case numbers

Patrol observation reports:
Suspicious incidents, persons, and vehicles; locations (field interview cards) and times

Missing person reports:
Name, address, telephone numbers, physical description, DOB

Warrants:
Name, charge, case number

Intelligence files
Name, address, telephone numbers, physical description, DOB, Social Security no., aliases, modus operandi

County Clerk's Office
Marital status, marriage license applications, addresses, (marriage licenses) dates of birth, signatures

County Clerk's Office
Full name and address, transcripts of preliminary hearings, (criminal files) probation officer's reports, subpoenas issued in the case, names of attorneys concerned

Department of Naturalization
Addresses of aliens, date of entry, manner of arrival, addresses, occupation, age, physical description

Credit Card Companies
Employment and credit references, types of charges (i.e., which hotels, gas stations, etc., are used)

County Assessor's Office
Full name and address, dimensions and taxable income of real property, improvement on property

County Tax Collector's Office
Full name and address, legal description of property, taxes paid on real and personal property, former owners of property

Building Departments
Cost of construction, blueprints, location of plumbing and wiring

Health Departments
Parents of a child, their occupations, their ages, mother's maiden name, name of physician

Welfare Departments
Case histories of persons on welfare

School Departments
Photograph, past and present student and teacher's records

State Department
Date of birth, photograph, description, occupation, dates (passport division) of anticipated foreign travel, vital statistics

County Records Office
Parents' ages, parents' occupations, mother's maiden (birth certificate section) name, name of delivering physician, date of birth, address when born, full name

Telephone Directories
Full name, address, phone number

Stockbrokers
Records of stock bought or sold, profits, and losses

Moving Companies
Forwarding address, inventory of property moved

Credit Reporting Agencies
Full name, address, date of birth, past and present occupation, present and former addresses, whether renting or buying, credit references, personal and business associates, marital status and relatives, location of banks and finance companies, business's worth, holdings, and ratings

Gas and Electric Companies
Full name and address, DOB, occupation, previous address of subject, persons previously living at same address

Water Companies
Full name and address, prior addresses, names of persons previously living at same address

Telegraph Companies
Occupation, copies of telegrams, money order information, possibly handwriting examples

American Medical Directory
Presidents and secretaries of all county medical associations, lists of hospitals and sanitariums with number of rooms and beds, doctors' names by street and city, medical schools and years of graduation, office addresses

Directory of Newspapers
Guide to newspapers and periodicals printed in the United and Periodicals, N.W. States and its possessions, thumbnail description of Ayer and Sons, every city, including population, county, and location Philadelphia with respect to nearest large city

Federal Immigration and Naturalization Service
Alien's addresses, date of entry, manner of arrival, occupation, age, physical description, marital status, children, signature, photograph

Department of Motor Vehicles:
Full name and address, description, marital status, registered owners, legal owners and description of vehicles, previous owners, operator's license numbers, thumbprints, abstracts of traffic citations, liens outstanding and lien holder

County Recorder's Office
Recorded deeds, grants, mortgages, encumbrances, wills admitted to probate, notices of mechanics' liens, powers of attorney

Newspaper Libraries/Morgues
Address, photograph, occupation, prior addresses of subject, names of persons previously living at same address, reputation of a business, back issues of city directories

Martindale-Hubbell
Biographical information on U.S. attorneys individually and Law Directory by law firm, education, representative clients

Federal Bureau of Investigation
Violent Criminal Apprehension Program (VICAP); and criminal profiling

Appendix T
Crime Analysis

General. Analysis of crime generally falls within two broad categories. One is to support specific investigative operations and the other to support resource utilization. This appendix will describe various types of crime analysis reports for these two categories.

General crime analysis types

a. Operational Crime Analysis. Crime analysis in support of operational decision making is a process of systematically examining crime incidents, criminal behaviors and characteristics, as well as other relevant events in an effort to achieve crime control goals through the implementation of appropriate strategies and tactics. Thus, the anticipated outcome of this type of analysis is to provide relevant information so as to plan action designed to fulfill tactical and strategic objectives.

b. Management analysis, on the other hand, does not focus only on crime data, but uses aggregate crime information, as well as many other data sources, in order to support administrative decisions relating to budgets, policy, staffing, capital improvements, inter- agency relations, etc.

Specific types of analysis functions

a. Tactical operational decision making.

(1) Crime series/pattern detection - A crime series may be defined as a number of offenses that are believed to be committed by the same person or group of persons. This relationship of offenses is identified by the discovery of similar characteristics that are unique to the perpetrator(s). In contrast, a crime pattern can be defined as a number of offenses that have some common characteristics, but not those that would be necessarily unique to a given person or group of persons. It is possible that the pattern is also a series; however, the common crime characteristics may simply be the type of target, geographic area, method of entry, type of property taken, time of day, etc. Early identification of a crime series could result in a fairly good description of the suspect(s) and/or a reasonable prediction of future crime targets. In either case, the objective of series analysis is apprehension. Pattern analysis, on the other hand, could yield data that may suggest other strategies such as validation or suppression.

(2) Suspect - crime correlations - Identifying perpetrators of known crimes has long been recognized as one of the major investigative tasks that can be aided by analysis. By systematically matching suspect physical, vehicle, or M.O. information from crime reports with similar information from offender based files,

a list of possible suspects may be constructed as investigative leads. The reverse of this process is also noteworthy. Starting with a suspect arrested for a given offense, a search of crime files indicates whether additional cases might be associated with the suspect. In this latter case, besides suspect physical, vehicle, or M.O. information, evidence related to the suspect may be one of the links connecting the arrested persons with the additional crime. Identifying recovered property as stolen, is a prime example of this function. Not only can this procedure help to clear more cases, it can also serve to strengthen prosecution efforts against the offender.

(3) Target - suspect profiles - Aside from attempting to forecast crime frequencies by time and area, there may exist a need to specify the nature of the objects that might be attacked. This effort requires a rather thorough description of the types of structures and/or persons victimized for a given crime problem. Target profiles might also include listings of typical crime scenes and corresponding MO's, as well as demographic and physical descriptions of the areas surrounding crime targets. Similarly, by applying this process to perpetrator data, suspect profiles can be constructed. Both types of profiles may help by focusing attention on most probable targets and suspects. With this knowledge, operational units will be better prepared to choose for implementation a variety of apprehension, suppression, and validation activities. Successfully employing a decoy tactic, for example, would presuppose that a rather accurate target profile was developed.

(4) Crime potential forecasts - As distinct from present or past crime problems, there may exist a need to determine future crime events. Although this forecasting will depend, primarily, on the historical analysis of cyclical, periodic, or special events, it will involve more than a straight line continuation of historical data. In order to identify these crime potentials, historical data must be viewed in the context of present and anticipated settings while focusing on probable locations, target types, and time ranges. Information from crime series/pattern analyses should aid immeasurably in predicting future target locations and times. For example, nighttime thefts from supply activities might be forecasted to rise significantly between pay periods, especially at those locations that border on areas where drug users are known to frequent. Another example might be the forecast of a crime potential occurring on paydays in certain areas.

b. Strategic operational decision making

(1) Exception reports - These types of reports are products designed to alert investigative and law enforcement personnel that the frequency of crime is above or below some pre-established limits. Based on the crime history for a given geographical location, a "normal" range of values (upper and lower thresholds) is computed for a specific crime type. Generally, seasonal fluctuations and special events should be taken into consideration while establishing thresholds. Care must be taken while determining appropriate time cycles for reporting. If the time

period is too short for the geographic area under study, crime frequencies will fluctuate too widely for thresholds to have much meaning.

(a) Upper threshold: When it is noted that a crime threshold is exceeded, a report is generated to trigger operational planning. If this planning effort determines that the situation is important enough to consider tactical deployment, further details concerning the crime problem will need to be presented and thus tactical level analysis will need to be accomplished.

(b) Lower threshold: With regard to the lower threshold, it is also valuable to know if a given area has experienced a decrease in crime frequencies over previous time periods. Such information can reveal whether a particular action plan is having its intended effect. Additionally, it can serve as a signal that resources may be redeployed to more needy areas.

(2) Crime trend forecasts - The forecasting of trends first requires an identification of the prevailing tendency, or general movement, of crime frequencies for a particular geographic area over a given period of time. The task is primarily a statistical one in which crime related data are projected into the future. For the most part, such projections are quite general, covering relatively large geographic areas and long time periods. Since the level of detail is much less an d the areas and long time periods are much greater than those used in forecasting crime potentials, trend analysis is therefore expected to show lower rates of error, but be less useful in tactical deployment. For example, forecasting that burglaries will increase 12% during the upcoming year may be more accurate, but less tactically useful than forecasting that a particular group will experience around a 20 to 30% increase in burglaries during the upcoming period between paydays.

(3) Resource allocation - Determining the most advantageous use of available manpower remains one of the major tasks of any investigative or law enforcement agency. Commanders and program managers are aided in this task when analysis units collect and analyze workload data in an effort to construct resource allocation models. In order to accomplish this task, the following variables should be analyzed:

(a) The demands for services, and the time expended to meet those demands.

(b) The manpower available to meet the mission and administrative demands.

(c) The assignment of manpower commensurate with the workload requirements.

(d) The allocation of assigned manpower in proportion to the frequency of the investigative service demands.

(e) The distribution of manpower allocated in such a way as it relates logically and rationally to the geography, and other special characteristics, of the investigative service demands.

(4) Situational analysis - The primary purpose of this analysis function is to better understand the characteristics of a given area and/or crime type. In contrast to a study of a particular crime problem for the purpose of tactical action, the aim of this function is to render background information (for a better "feel") of the underlying factors and dynamics associated with crime occurrences. In many ways this will result in a kind of "sociological profile", and takes two basic forms: area-specific and crime-specific.

(a) An area-specific analysis will usually focus on a relatively small geographic area and describe its physical and demographic characteristics together with its crime history.

(b) Crime-specific analysis, on the other hand, will take a selected crime type and, over several geographical areas, attempt to specify the particular characteristics associated with that crime type. The classes of variable s typically employed in this level of analysis involve victim and suspect physical and social characteristics, their interactions, their environments, as well as the ecology of the crime scene, and so on.

c. Management decision making.

(1) Cost/effectiveness reports - This analysis function requires not only the analysis of crime related data, but also that such data be linked in a meaningful way to organizational inputs. Typical inputs are manpower, money, equipment, and facilities. Often times, however, reports of this type should involve more than ratios of inputs to crime rates; they frequently require an in-depth analysis of the efforts made toward achieving crime related goals. This necessitates some specification of productivity and measurement (both process and outcome measures). A report listing how the present level of productivity compares with what other alternatives would cost is an example of this function. Another example would be a zero based budget report for the operational elements.

(2) Program evaluations - This function relates to the use of crime data for the purpose of assessing the merits of policies, procedures, and projects; that is, to determine if specific activities are working as intended. These activities (independent variables) are compared with changes in outcome measures (dependent variables), which frequently take the form of crime and arrest data. This analysis function approaches formal hypothesis testing and, thus, often suggests the use of experimental methodology. In order to determine whether a

particular tactic reduces the level of robberies, for example, there should not only be a before - after comparison of crime frequencies, but also should be a determination if comparison areas (control groups) were similarly affected. Typically, inferential statistics will need to be employed in order to reach valid conclusions.

(3) Support studies - The primary purpose of this analysis function is to provide empirically based recommendations where intuition, speculation, tradition, or political philosophy have previously dominated administrative decision ma king. At this level of analysis rarely do "the statistics speak for themselves." On the contrary, studies of this type often require the analyst to make recommendations with a reasonable expectation that they will meet with some opposition. It is incumbent upon the analyst, then, to determine what assumptions are in play, limitations of the source data, and methodological problems encountered. Products resulting from this analysis function can range from formal staff - studies on changes in laws to recommendations for the changes in operating procedures. In any case, it would behoove the analyst to know what decisions will be made as a result of the request for information. He or she may have to defend their efforts.

Appendix U
Reference Publications

AR 1-4, 10 March 1986
Employment of DA Resources in Support of the U.S. Secret Service

AR 1-201, 17 March 1993
Army Inspection Policy

AR 10-87, 30 October 1992
Major Army Commands in the Continental United States

AR 11-2, 1 August 1994
Management Control

AR 19-57

AR 20-1, 29 March 2002
Inspector General Activities and Procedures

AR 25-1, 31 May 2002
Army Information Management

AR 25-30, 15 May 2002
The Army Publishing Program

AR 25-55, 1 November 1997
The Department of the Army Freedom of Information Act Program

AR 25-400-2, 1 October 2001
The Modern Army Record Keeping System (MARKS)

AR 27-10, 20 August 1999
Military Justice

AR 27-40, 19 September 1994
Litigation

AR 40-12, 24 January 1992
Quarantine Regulations of the Armed Forces

AR 40-2

AR 40-31, 4 June 1993
Armed Forces Institute of Pathology and Armed Forces Histopathology Centers

AR 40-66, 3 May 1999
Medical Record Administration and Health Care Documentation

AR 70-1, 15 December 1997
Army Acquisition Policy

AR 190-52

AR 190-6, 15 January 1982
Obtaining Information from Financial Institutions

AR 190-9, 24 July 1992
Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies

AR 190-11, 12 February 1998
Physical Security of Arms, Ammunition, and Explosives

AR 190-13, 30 September 1993
The Army Physical Security Program

AR 190-14, 13 March 1993
Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

AR 190-22, 1 January 1993
Searches, Seizures, and Disposition Property

AR 190-27, 28 May 1993
Army Participation in the National Crime Information Center

AR 190-29, 1 March 1984
Misdemeanors and Uniform Violation Notices Referred to U.S. Magistrates or District Courts

AR 190-30, 1 June 1978
Military Police Investigations

AR 190-41, 1 March 1994
Customs Law Enforcement

AR 190-45, 20 October 2002
Military Police Law Enforcement Reporting

AR 190-48,
Protection of Federal Witnesses on Active Army Installations

AR 190-53, 3 November 1986
Interception of Wire and Oral Communications for Law Enforcement Purposes With USACIDC Supplement

AR 190-58, 22 March 1989
Personal Security

AR 195-1, 12 August 1974
Army Criminal Investigation Program

AR 195-2, 30 October 1985
Criminal Investigation Activities

AR 195-3, 22 April 1987
Acceptance, Accreditation, and Release of U.S. Army Criminal Investigation Command Personnel

AR 195-4, 15 April 1983
Use of Contingency Limitation .0015 Funds for Criminal Investigative Activities With USACIDC Supplement

AR 195-5, 28 August 1992
Evidence Procedures

AR 195-6, 29 September 1995
Department of the Army Polygraph Activities

AR 195-7, 11 March 1985
Criminal Investigation Support to the Army and Air Force Exchange Service

AR 335-15, 28 October 1986
Management Information Control System

AR 340-21, 5 July 1985
The Army Privacy Program

AR 350-1, 1 August 1981
Army Training

AR 350-30, 10 December 1985
Code of Conduct/Survival, Evasion, Resistance and Escape

AR 360-1, 15 September 2000
The Army Public Affairs Program

AR 360-81, 20 October 1989
Command Information Program

AR 380-5, 29 September 2000
Department of the Army Information Security Program

AR 380-13
Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations

AR 380-19, 27 February 1998
Information Systems Security

AR 380-67, 9 September 1988
Personnel Security Program

AR 381-10, 1 July 1984
U.S. Army Intelligence Activities

AR 381-12, 15 January 1993
Subversion and Espionage Directed Against the U.S. Army (SAEDA)

AR 381-20, 15 November 1993
The Army Counterintelligence Program

AR 381-100
U.S. Army Human Intelligence Collection Programs

AR 385-40, 1 November 1994
Accident Reporting and Records

AR 525-13, 4 January 2002
Antiterrorism

AR 5-9, 16 October 1998
Area Support Responsibilities

AR 530-1, 15 Oct 95
Operations Security

AR 600-8, 1 October 1989
Military Personnel Management

AR 600-8-1, 20 October 1994
Army Casualty Operations/Assistance/Insurance

AR 600-8-24, 21 July 1995
Officer Transfers and Discharges

AR 600-63, 28 April 1996
Army Health Promotion

AR 600-85, 1 October 2001
Army Substance Abuse Program

AR 600-9, 1 September 1986
The Army Weight Control Program

AR 621-108, 3 March 1992
Military Personnel Requirements for Civilian Education

AR 635-200, 1 November 2000
Enlisted Personnel

AR 710-2, 31 October 1997
Inventory Management Supply Policy Below the Wholesale Level

AR 735-5, 31 January 1998
Policies and Procedures for Property Accountability

AR 930-5, 19 November 1969
American National Red Cross Service Program and Army Utilization

DA Pam 25-51, 30 April 1999
The Army Privacy Program-System Notices and Exemption Rules

DA Pam 351-4, 31 October 1995
U.S. Army Formal Schools Catalog

DA Pam 710-2-1, 31 December 1997
Using Unit Supply System (Manual Procedures)

DA Pam 738-750, 1 August 1994
Functional Users Manual for the Army Maintenance Management System

DoD 0-2000.12-H
Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence

DoDM 4525.6M
DoD Postal Manual (Volume 1 and Volume 2)

DoDM 5100.76M
Physical Security of Sensitive Conventional AA&E

DoDM 5505.4
Defense Investigative Management Information System

DoDD 5040-1 (Rescinded)

DoDD 5040.2R (Rescinded)

DoDD 5040.2, 11 Oct 85
Visual Information (VI)

DoDD 5040-3, 5 Dec 85
DoD Joint Visual Information Services

DoDD 5220.22
Industrial Security Regulation

DoDR 5220.22-R
Industrial Security Regulation

DoDD 5500.7
Standards of Conduct

DoDR 5500.7-R
Joint Ethics Regulation

DoDD 5525.7
Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigation and Prosecution of Certain Crimes

DoDD 7050-5
Coordination of Remedies for Fraud and Corruption Related to Procurement Activities

DoDI 5240.4
Reporting of Counterintelligence and Criminal Violations

DoDI 5505.7
Titling and Indexing of Subjects in Criminal Investigations in the Department of Defense

DoD Policy (Memorandum Number 5)
Criminal Drug Investigative Activities

MCM, 1 October 1998
Manual for Courts Martial

5 USC 552
Freedom of Information Act

5 USC 552a
Privacy Act

FM 19-20, 25 Nov 85
Law Enforcement Investigations

FM 21-20
Physical Fitness Training

FC 19-136
Protective Services

CIDR 10-1
USACIDC Command Structure

CIDR 10-2
USACIDC Organization and Functions

CIDR 1-201
Organizational Inspection Program

CIDR 25-1
Microcomputers, Microcomputers Policies, Procedures and Standards

CIDR 70-1
Evaluation and Acquisition of USACIDC Equipment

CIDR 195-28
Polygraph Activities

CIDR 710-5
Materiel Management System

CIDR 385-1

CIDP 195-7
Personal Security Assessment Briefings

CIDP 190-53
Electronic Surveillance

CIDP 710-1
USACIDC Catalog of Investigative Equipment

CIDM 25-55
Coordination of Freedom of Information and Privacy Act Requests which have Media Interest

USC
United States Code

FRCP
Federal Rules of Criminal Procedure