FM 2-22.2 (FM 34-60)

Counterintelligence

October 2009

Headquarters, Department of the Army

This publication is available at:

Army Knowledge Online
(www.us.army.mil)

General Dennis J. Reimer
Training and Doctrine Digital Library
(http://www.train.army.mil)

United States Army Publishing Agency
(http://www.army.mil/usapa)

Field Manual
No. 2-22.2 (34-60)

Headquarters
Department of the Army
Washington, DC, 21 October 2009

Counterintelligence

Contents

Page

PREFACE ..... **vii**

Chapter 1 COUNTERINTELLIGENCE MISSION, STRUCTURE, AND ORGANIZATION **1-1**
Army Counterintelligence 1-1
Counterintelligence Special Agent 1-1
Tenets of Counterintelligence 1-1
Counterintelligence Core Competencies 1-3
Counterintelligence Mission 1-4
Counterintelligence Structure 1-5
2X 1-6
Counterintelligence Coordinating Authority 1-7
U.S. and Department of Defense Counterintelligence Community 1-13
Army Counterintelligence Levels of Employment 1-14

Chapter 2 COUNTERINTELLIGENCE INVESTIGATIONS **2-1**
Investigative Personnel 2-1
Counterintelligence Investigation Objectives 2-1
Investigative Authority 2-2
Counterintelligence Investigative Jurisdiction 2-3
Incidents of Counterintelligence Interest 2-4
Counterintelligence Investigative Control and Oversight 2-6
Counterintelligence Investigation Types and Categories 2-7
Investigative Process 2-10
Records Checks 2-21
Counterintelligence Interviews 2-27
Counterintelligence Investigative Reports and Files 2-43

***This publication supersedes FM 34-60, 3 October 1995.**

Chapter 3 COUNTERINTELLIGENCE OPERATIONS 3-1
General 3-1
Advice and Assistance Programs 3-1
Covering Agent Program 3-2
Counterintelligence Support to Research and Technology Protection 3-2
Counterintelligence Support to Acquisition and Special Access Programs 3-3
Counterintelligence Red Team Operations 3-3
Counterintelligence Support to Treaty Verification 3-4
Counterintelligence Support to Antiterrorism and Protection 3-4
Threat Assessments and Vulnerability Assessments 3-5
Counterintelligence Support to Homeland Defense and Civil Support Operations 3-6
Counterintelligence Support to Joint Terrorism Task Force 3-7
Counterintelligence Support to Counterdrug Operations 3-7
Counterintelligence Support to Information Superiority 3-7
Counterintelligence Support to Military Deception 3-8
Counterintelligence Support to Psychological Operations 3-9
Counterintelligence Support to Electronic Warfare 3-9
Counterintelligence Support to Operations Security 3-10
Counterintelligence Support to Counterpropaganda 3-10
Counterintelligence Support to Counterdeception 3-11
Counterintelligence Support to Physical Security 3-11
Counterintelligence Support to Physical Destruction 3-11
Counterintelligence Support to Information Assurance 3-12
Counterintelligence Support to Civil-Military Operations 3-12
Counterintelligence Support to Public Affairs 3-13
Counterintelligence Support to Computer Network Operations 3-13

Chapter 4 COUNTERINTELLIGENCE COLLECTION PROGRAM 4-1
General 4-1
Counterintelligence Collection Program 4-2
Counterintelligence Debriefings, Screening, and Liaison 4-3
Control of Source Information 4-10
Unit Counterintelligence Requirements Management 4-11
Standing Counterintelligence Collection Requirements 4-12
Counterintelligence Support to Threat and Vulnerability Assessments 4-12

Chapter 5 ANALYSIS, TOOLS, AND PRODUCTION 5-1
General 5-1
Anomalies, Signatures, and Patterns 5-3
Counterintelligence Threat Analysis 5-3
Counterintelligence Support to Intelligence Preparation of the Battlefield 5-5
Counterintelligence Operational Analysis 5-8
Analytical Tools 5-9
Production 5-20

Chapter 6 TECHNICAL COUNTERINTELLIGENCE SERVICES AND SUPPORT 6-1
Technical Investigative Techniques 6-1
Electronic Surveillance 6-1
Investigative Photography and Video Recording 6-2
Laboratory Analysis 6-2
Polygraph Support 6-2
Technical Surveillance and Countermeasures Program 6-5
Deception Identification and Detection (Biometrics) 6-7
Computer Forensics 6-8
Support to Information Tasks (Computer Network Operations) 6-9

Chapter 7 CYBER COUNTERINTELLIGENCE 7-1
General 7-1
Cyber Counterintelligence Support to Core Functions 7-1
Cyber Threat Briefings 7-5
Computer Network Incident Categories 7-6
Cyber Indicators of Counterintelligence Interest 7-8
Recognizing Potential Evidence 7-9
Search and Seizure 7-9

Chapter 8 INVESTIGATIVE LEGAL PRINCIPLES 8-1
Intelligence Oversight 8-1
Jurisdiction 8-2
Criminal Law 8-4
Evidence 8-5
Rights Amendment 8-8
Investigative Authority 8-12
Crimes and Incidents Within Counterintelligence Investigative Jurisdiction 8-16

Chapter 9 COUNTERINTELLIGENCE REPORTING 9-1
Tenets of Reporting 9-1
Reports Management 9-1
Report Categories 9-2
Reporting Architecture 9-4
Information Sharing and Release 9-6

Appendix A COUNTERINTELLIGENCE PROGRAM ADMINISTRATION A-1

Appendix B CONTRACTOR SUPPORT TO COUNTERINTELLIGENCE ACTIVITIES B-1

Appendix C INTERPRETER SUPPORT TO COUNTERINTELLIGENCE ACTIVITIES C-1

Appendix D FBI DELIMITATIONS AGREEMENT D-1

Appendix E COUNTERINTELLIGENCE INVESTIGATIVE REPORT WRITING GUIDE E-1

Appendix F PREDEPLOYMENT AND MISSION PLANNING F-1

Appendix G COUNTERINTELLIGENCE SUPPORT TO MULTINATIONAL OPERATIONS G-1

Appendix H AUTOMATION, COMMUNICATION, AND EQUIPMENT H-1

Appendix I COUNTERINTELLIGENCE SPECIAL AGENT APPLICATION INFORMATION PACKET I-1

Appendix J UNIT CUSTODIAN BADGE AND CREDENTIALS HANDBOOK J-1
GLOSSARY Glossary-1
REFERENCES References-1
INDEX Index-1

Figures

Figure 1-1. Neutralization versus exploitation 1-2
Figure 1-2. 2X organization 1-7
Figure 2-1. Investigative life cycle 2-11
Figure 2-2. Indicators of espionage 2-13
Figure 2-3. Example of an interview room setup 2-33
Figure 3-1. Counterintelligence operations 3-2
Figure 3-2. Counterintelligence support to Army information tasks 3-8
Figure 5-1. Intelligence process 5-1
Figure 5-2. Example of a time event chart 5-10
Figure 5-3. Analysis Notebook theme line chart 5-10
Figure 5-4. Example of an association matrix 5-11
Figure 5-5. Example of an association matrix symbology 5-11
Figure 5-6. Example of an activities matrix 5-12
Figure 5-7. Example of a link analysis diagram 5-13
Figure 5-8. Example showing deceased person 5-14
Figure 5-9. Example of person with suspected alias 5-14
Figure 5-10. Example of person with confirmed alias 5-14
Figure 5-11. Example of nonpersonal entity 5-14
Figure 5-12. Confirmed linkage 5-14
Figure 5-13. Suspected linkage 5-15
Figure 5-14. Legend on connectivity line 5-15
Figure 5-15. Connectivity between persons 5-15
Figure 5-16. Example of mutually associated members 5-16
Figure 5-17. Connection between organizations and events 5-16
Figure 5-18. Connectivity between persons but not the organization 5-17
Figure 5-19. Association with an entity 5-17
Figure 5-20. Person with greatest number of personal associations 5-17
Figure 5-21. Person with next highest number of personal associations 5-18
Figure 5-22. Confirmed personal associations 5-18
Figure 5-23. Example of activities, organization, and nonpersonal entities 5-18
Figure 5-24. Analyst Notebook link diagram showing information from an activity matrix 5-19
Figure 5-25. Analyst Notebook link diagram showing nonpersonal relationship 5-19

Figure 5-26. Analyst Notebook hierarchy layout 5-20
Figure 9-1. Reporting architecture 9-5
Figure D-1. FBI delimitations agreement contents D-1
Figure E-1. Example of a CI incident report E-16
Figure E-2. Example of an IMFR—interview E-24
Figure E-3. Example of an IMFR—personnel files checks E-35
Figure E-4. Example of an IMFR—records checks E-39
Figure E-5. Example of an IMFR—intelligence files checks E-41
Figure E-6. Example of an IMFR—law enforcement records checks E-43
Figure E-7. Example of a transmittal letter for an ROI E-51
Figure E-8. Example of an ROI E-52
Figure E-9. Example of an SOI E-55
Figure E-10. Privacy Act of 1974 advisement statement E-57
Figure E-11. Perjury warning E-58
Figure E-12. Secrecy affirmation statement E-59
Figure F-1. Appendix 3 (CI) to Annex B (Intelligence) to an OPORD F-4
Figure I-1. Information sheet—CI (MOS 35L) I-2
Figure I-2. Applicant information sheet I-7
Figure I-3. CI special agent application—minimum qualifications I-9
Figure I-4. CI applicant processing checklist I-11
Figure I-5. CI special agent applicant interview process I-12
Figure I-6. Orientation statement I-14
Figure I-7. Instructions for the contingency statement and compositions I-16
Figure I-8. Final interview I-18
Figure I-9. Final interview guide I-19
Figure I-10. CI applicant interview biographic sheet I-22
Figure I-11. Interviewing agent's post-interview requirements I-32
Figure I-12. Statement of interview I-33
Figure I-13. CI applicant HRC memorandum I-38
Figure J-1. Email receipt for badge and credentials materials shipped to a unit J-3
Figure J-2. Email receipt for CI badge and credentials hand-carried to a unit J-4
Figure J-3. Email 1 example—hand-carry transfer coordination process J-6
Figure J-4. Email 2 example—gaining unit responds to the initial email J-7
Figure J-5. Email 3 example—hand-carry authorization email from ITRADS J-7
Figure J-6. Email 4 example—gaining unit receipts for the badge and credentials J-7
Figure J-7. Email 5 example—ITRADS acknowledgment of transfer J-8
Figure J-8. Unit badge and credentials inventory memorandum format J-9
Figure J-9. Receipt and responsibility statement format J-11
Figure J-10. Example of badge and credentials return memorandum format J-13
Figure J-11. Badge and credentials request memorandum format J-14

Figure J-12. Request for USAI representative credentials J-15
Figure J-13. Misuse of badge and credentials materials—initial report format..... J-16
Figure J-14. Misuse of badge and credentials materials—final report format J-17
Figure J-15. Loss of badge and credentials materials—initial report format J-18
Figure J-16. Loss of badge and credentials materials—final report format J-19
Figure J-17. Additional duty appointment badge and credentials custodians J-20
Figure J-18. Request to establish a USAI badge and credentials account J-21
Figure J-19. Request for revalidation of badge and credentials account J-23

Tables

Table 1-1. Counterintelligence coordinating authority functions 1-8
Table 1-2. Operations support cell functions 1-10
Table 1-3. Operational management team functions..... 1-10
Table 1-4. Counterintelligence team functions 1-12
Table E-1. Personal data E-2
Table E-2. Military ranks and civilian titles E-4
Table E-3. Physical description..... E-4

Preface

This manual provides doctrinal guidance, techniques, and procedures for the employment of counterintelligence (CI) special agents in the Army. It outlines—

- CI investigations and operations.
- The CI special agent's role within the intelligence warfighting function.
- The importance of aggressively countering foreign intelligence and security services (FISS) and international terrorist organizations (ITO).
- The roles and responsibilities of those providing command, control, and technical support to CI investigations and operations.
- The need for effective dissemination of CI reports and products and the importance of cross-cueing other intelligence disciplines.
- The significance of cultural awareness as a consideration to counter the foreign intelligence threat.

This manual expands upon the information in FM 2-0 and supersedes FM 34-60. It is consistent with doctrine in FM 3-0, FM 5-0, FM 100-15, and JP 2-0. When published, FM 2-22.2 will provide further information on CI activities when Army forces are employed in tactical operations.

This manual provides the doctrinal guidance for CI special agents, commanders, and staffs of the military intelligence organizations responsible for planning and executing CI missions. It also serves as a reference for personnel developing doctrine and tactics, techniques, and procedures; materiel and force structure; institutional and unit training; and standing operating procedures for CI activities at all Army echelons.

FM 2-22.2 is intended for use by CI special agents, commanders, staff officers, military intelligence personnel, and Government civilian and contract employees charged with responsibility for CI activities and operations. It is also intended for commanders and staffs of joint and multinational commands, U.S. Naval and Marine forces, units of the U.S. Air Force, and the military forces of multinational partners. This manual applies to the spectrum of conflict and operational themes.

This manual applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve unless otherwise stated, and Federal employees and contractor personnel employed by the Services to engage in CI activities.

For the purposes of this manual, the term special agents or agents refers to an enlisted Soldier in military occupational specialty 35L, a warrant officer in WO area of concentration (AOC) 351L, a commissioned officer in AOC 35E, or their Federal civilian employee counterpart.

Headquarters, U.S. Army Training and Doctrine Command is the proponent for this publication. The preparing agency is the U.S. Army Intelligence Center and Fort Huachuca. Send written comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, ATZS-CDI-D (FM 2-22.2), U.S. Army Intelligence Center, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017: by email to ATZS-FDC-D@conus.army.mil or submit an electronic DA Form 2028.

This page intentionally left blank.

Chapter 1

Counterintelligence Mission, Structure, and Organization

Counterintelligence is information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities (EO 12333).

Counterintelligence (CI) includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of adversaries. It is a key intelligence community contributor to protect U.S. interests and equities.

ARMY COUNTERINTELLIGENCE

1-1. CI focuses on negating, mitigating, or degrading the foreign intelligence and security services (FISS) and international terrorist organizations (ITO) collection threat that targets Army interests through the conduct of investigations, operations, collection, analysis, production, and technical services and support.

1-2. CI analyzes the threats posed by FISS and the intelligence activities of nonstate actors such as organized crime, terrorist groups, and drug traffickers. CI analysis incorporates all-source information and the results of CI investigations and operations to support a multidiscipline analysis of the force protection threat.

COUNTERINTELLIGENCE SPECIAL AGENT

1-3. The CI special agent has the distinct mission of detecting, identifying, countering, and neutralizing FISS and ITO threats directed towards the Army through the execution of all CI functions. CI special agents should not be confused with human intelligence (HUMINT) collectors, military occupational specialty (MOS) 35M, and warrant officer (WO) area of concentration (AOC) 351M. They are specifically trained and certified for, tasked with, and engage in the collection of information from individuals (HUMINT sources) for the purpose of answering HUMINT-specific requirements. Although CI and HUMINT personnel may use similar methods, their missions are separate and distinct. Commanders should not use them interchangeably. Using CI personnel for HUMINT missions degrades the Army's ability to protect its forces, information, and critical technology that provides the Army operational and technological superiority over existing and future adversaries.

Note. For the purpose of this FM, a CI special agent consists of enlisted personnel in MOS 35L, WOs in AOC 351L, commissioned officers in AOC 35E, and their Federal civilian employee counterparts.

TENETS OF COUNTERINTELLIGENCE

1-4. The National Security Act of 1947, codified under Title 50, USC § 401a, designates CI as an intelligence activity. While one of the CI cornerstones is the conduct of investigations, Title 50, USC highlights—the best long-term solution to counter the FISS and ITO collection threats is offensively exploiting the situation to identify all the participants, and undermining the FISS and ITO's ability to collect effectively on Army equities through control of the participants and information. Neutralization of a

FISS and ITO threat through exposure, changes to systemic procedures, or criminal prosecution should always be the secondary consideration. Neutralization inhibits Army CI's ability to fully identify all the participants and assess the damage caused to national security; however, all CI investigative activities should be conducted at a prosecutorial standard to preserve the legal integrity and admissibility of evidence. Figure 1- 1 shows criminal versus intelligence approach to CI operations.

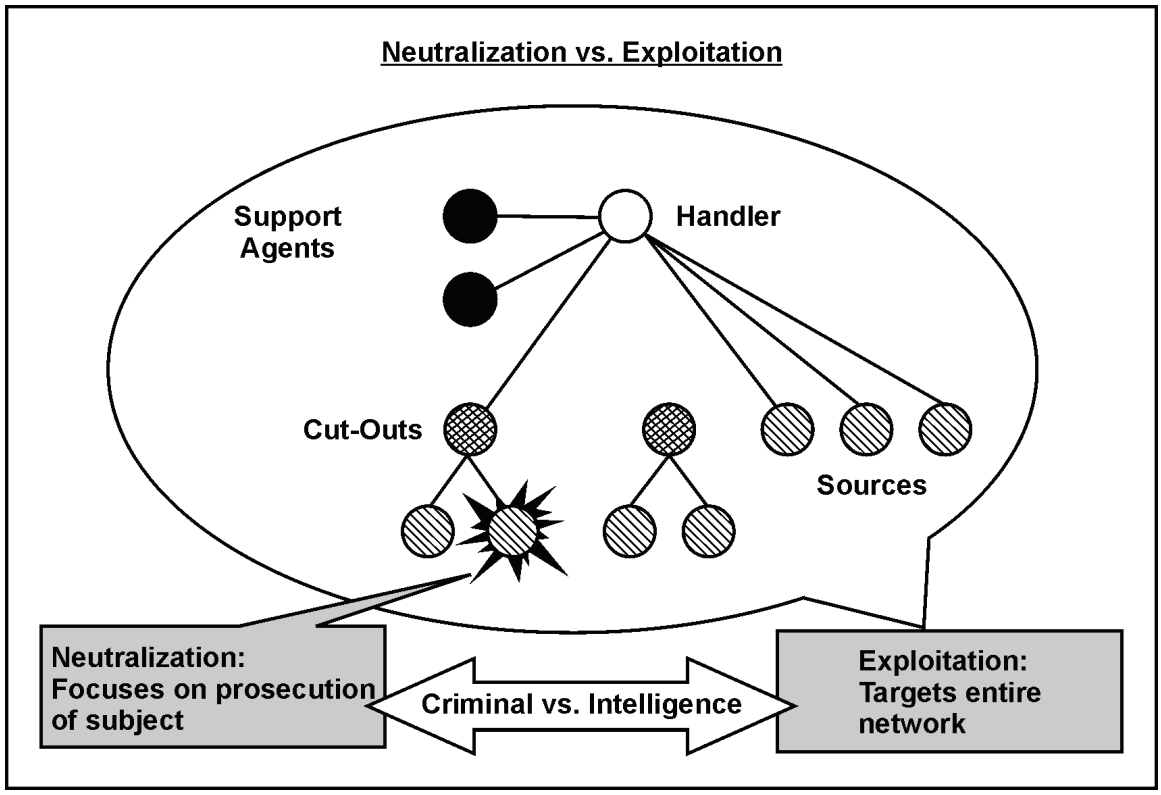

Figure 1-1. Neutralization versus exploitation

1-5. The Department of Defense (DOD) defines CI as a multidiscipline function to counter the full range of FISS and ITO collection activities. However, the only FISS and ITO intelligence platform that Army CI can offensively and proactively counter is their HUMINT capability. Signals intelligence, imagery intelligence, or other technical collection activities are generally standoff platforms. CI can only provide assessments on the capabilities and make recommendations for countermeasures to mitigate the threats. The facts presented make Army CI focused generally on counter-HUMINT activities.

1-6. CI is the fusion of intelligence, security, and law enforcement functions into a single element that thinks like a FISS and ITO entity, and employs a broad range of functions to protect Army personnel, property, information, operational intentions, and critical technologies. This ensures operational and technological superiority over existing and future adversaries. Although proper CI employment protects national defense information, proper CI employment can also undermine the adversaries' understanding and knowledge of U.S. policies and objectives and make them react predictably if Army CI can effectively control the adversary's abilities to collect against U.S. interests. The following elements support the different CI objectives:

- Intelligence (exploitation)—CI sensitive and investigative source operations.
- Security (deter, detect, identify, counter)—advice and assistance, briefings, debriefings, screenings, security program inspections.
- Law enforcement (neutralize)—CI investigations.

COUNTERINTELLIGENCE CORE COMPETENCIES

1-7. CI core competencies are interrelated, mutually supporting, and can be derived from one another. No single competency can defeat the FISS and ITO intelligence collection threat targeting U.S. interests, in general, and Army interests, specifically. The CI core competencies include—

- Operations.
- Investigations.
- Collection.
- Analysis and production.
- Intelligence analysis.
- Operational analysis.

OPERATIONS

1-8. CI operations are broadly executed CI activities that support a program or specific mission. CI operations use one or more of the core CI competencies discussed below. CI operations can be offensive or defensive, and they are derived from, transitioned to, or used simultaneously—depending on the scope, objective, or continued possibility for operational exploitation. CI operations fall into two categories: CI support operations and CI sensitive operations.

INVESTIGATIONS

1-9. CI investigations are conducted when national security crimes are allegedly committed by anyone under CI authority. The primary objective of any CI investigation is the identification, exploitation, or neutralization of threats directed against the Army. CI investigations are also conducted to identify systemic security problems that may have damaging repercussions to Army operations and national security interests.

COLLECTION

1-10. CI collection is the systematic acquisition of information concerning the FISS and ITO intelligence collection threat targeting Army equities. CI elements conduct collection activities to support the overall CI mission. CI collection is conducted by using sources, elicitation, official liaison contacts, debriefings, screenings, and open-source intelligence to obtain information that answers the standing counterintelligence collection requirements (SCICRs) or other collection requirements based upon commanders' requirements. Although CI and HUMINT have a collection mission, there are distinct differences between their collection objectives. HUMINT focuses on answering the commander's critical information requirements (CCIRs) concerning the plans, intentions, capabilities, and disposition of the adversary, as a whole.

1-11. CI specifically targets the FISS and ITO intelligence collection threat targeting U.S. forces. CI collection is conducted to understand how FISS and ITO are targeting U.S. forces, so countermeasures can be identified and recommended to commanders and program managers to protect personnel, mission, resources, and technology. Collection is only one of five CI functions; whereas, collection is HUMINT's only mission.

ANALYSIS AND PRODUCTION

1-12. CI analysis is used to satisfy the supported commander's intelligence requirements and to provide focus and guidance to CI operations. CI analysis and production can be accomplished at any level in which Army CI assets are assigned to counter the FISS and ITO collection threat; support protection of U.S. personnel, property, and operations; protect the research and development of critical technologies; and support Army information tasks to protect U.S. forces information systems.

Intelligence Analysis

1-13. CI analysis provides the supported commander with situational awareness and understanding of the operational environment. CI analysis should be focused on predictive assessments of FISS and ITO plans, intentions, and capabilities. This allows the commander to make informed decisions on the protection posture and targeting to neutralize or exploit those threats to the advantage of U.S. forces. Accurate CI analysis also increases the visibility of proactive and effective CI support and establishes credibility with the supported commander. This in turn leads the commander to trust and rely upon the CI assets and often give them more flexibility to execute CI operations.

Operational Analysis

1-14. Operational analysis allows the operational management elements (2X, counterintelligence coordinating authority [CICA] and operational management team [OMT] leaders) to gauge the effectiveness and success of their subordinate operational CI teams. This is done through assessments on source production (quantity and quality), source vetting (reliability, accuracy, response to control), and requirements coverage. Operational analysis also allows operational managers to deconflict CI operations and to provide direction and focus to eliminate redundancy and/or increase the efficiency of the CI teams.

TECHNICAL SERVICES AND SUPPORT

1-15. CI technical services are used to assist the CI core competencies of investigations, collections, and operations or to provide specialized technical support to a program or activity. The proliferation of sophisticated collection technology, surveillance, and "eaves-dropping" devices available in the commercial markets enable any FISS and ITO with the ability to increase their capability and effectiveness in collecting on Army interests.

1-16. To mitigate this increasing threat requires a specialized expertise. CI organizations with technically trained CI special agents are chartered with providing this unique technical capability to augment and provide specialized support to the CI mission. This includes CI special agents trained to—

- Perform technical surveillance countermeasures (TSCM).
- Perform cyber CI activities that provide protection to information networks as well as identify vulnerabilities and attempted intrusions into Army and DOD computer networks.
- Perform CI scope polygraph examinations.
- Provide support to Army information tasks.

COUNTERINTELLIGENCE MISSION

1-17. The mission of Army CI is to conduct aggressive, comprehensive, and coordinated operations, investigations, collection, analysis and production, and technical services. This CI mission is conducted worldwide to detect, identify, assess, counter, exploit, or neutralize the FISS and ITO collection threat to the Army and DOD to protect the lives, property, or security of Army forces. Army CI has four primary mission areas:

- Counterespionage (CE).
- Support to protection.
- Support to research and technology protection (RTP).
- Cyber CI.

COUNTERESPIONAGE

1-18. CE detects, identifies, counters, exploits, or neutralizes the FISS and ITO collection threat targeting Army and DOD equities or U.S. interests. CE programs use both investigations and collection operations to

conduct long-term operations to undermine, mitigate, or negate the ability of FISS and ITO to collect effectively on Army equities. CE programs also affect the adversarial visualization and decisionmaking concerning the plans, intentions, and capabilities of U.S. policy, goals, and objectives. The goal of CE is to—

- Limit the adversary's knowledge of U.S. forces, plans, intentions, and capabilities through information denial.
- Limit the adversary's ability to target effectively U.S. forces by disrupting their collection capability.

COUNTERINTELLIGENCE SUPPORT TO PROTECTION

1-19. CI support to protection ensures the survivability and mission accomplishment of Army and DOD forces.

1-20. CI's objective in supporting protection is to—

- Limit the compromise and exploitation of personnel, facilities, operations, command and control (C2), and operational execution of U.S. forces.
- Negate, mitigate, or degrade adversarial planning and targeting of U.S. forces for exploitation or attack.
- Support the war on terrorism.

SUPPORT TO RESEARCH AND TECHNOLOGY PROTECTION

1-21. Support to RTP is focused on preventing the illegal diversion or loss of critical technology essential to the strategic advantage of the U.S.

1-22. CI's objective in supporting RTP is to—

- Protect critical technology information from adversarial countermeasures development.
- Ensure U.S. technological overmatch against existing and future adversaries.

CYBER COUNTERINTELLIGENCE

1-23. Cyber CI protects information networks and provides an offensive exploitation capability against adversarial networks to ensure information superiority of U.S. forces.

1-24. CI's objective in conducting cyber CI activities is to—

- Maintain U.S. forces information dominance and superiority over existing and future adversaries.
- Protect critical information networks from adversarial attack or exploitation.
- Undermine adversarial information operations, systems, and networks.

COUNTERINTELLIGENCE STRUCTURE

1-25. CI organizations and Army force structure are designed to support the modular force construct through scalable teams, operations management, and technical control packages. CI elements assigned to battlefield surveillance brigades, divisions, corps, Army Service component commands (ASCCs), and strategic units are capable of operating at all echelons and throughout full spectrum operations. The joint 2X organizational and operational concept has been established in Army force structure to decentralize CI operational approval and execution. As the primary force provider for the DOD CI in contingency and combat operations, the establishment of the 2X and the CICA throughout the Army ensures a trained and

experienced cadre of CI professionals capable of filling Army, joint, and combined 2X and CICA/task force CI coordinating authority (TFCICA) positions.

2X

Note. 2X denotes the 2X staff officer at all echelons—S-2X (brigade), G-2X (division, corps, ASCC), J-2X (joint task force), C-2X (combined task force), and Army G-2X (Department of the Army [DA] level).

1-26. The 2X is the CI and HUMINT manager authorized to coordinate, deconflict, and synchronize all CI and HUMINT missions in the area of operations (AO). The 2X manages CI and HUMINT intelligence requirements including HUMINT collection requirements, time-sensitive collection requirements, report evaluations with source-directed requirements, and source assessments. Although the 2X section may be structured differently at each echelon, there is always a requirement for three components—CICA, a HUMINT operations cell (HOC), and an operations support cell (OSC). Figure 1-2 provides a graphic depiction of the 2X organization. The 2X is responsible for—

- Participating in predeployment or deployment planning for CI and HUMINT assets to support operations.
- Coordinating, through the HOC and CICA/TFCICA, all CI and HUMINT activities to support intelligence collection and the intelligence aspects of protection for the deployed commander.
- Managing collection requirements for CI and HUMINT in coordination with intelligence, surveillance, and reconnaissance (ISR) synchronization.
- Providing specific CI and HUMINT collection plans to the collection manager for integration into the ISR plan.
- Coordinating and deconflicting all CI and HUMINT operations within the AO.
- Serving as the release authority for CI and HUMINT reporting.
- Releasing reports to the Distributed Common Ground System-Army (DCGS-A) only after ensuring all technical control measures for reporting have been met.

1-27. The 2X is a commissioned officer with a CI or HUMINT AOC (35E/F). Within joint and combined force commands, the J/C-2X may be either an Army, Navy, Air Force or Marine Corps officer or civilian depending upon the requirements of the approved joint manning document. (See TC 2-22.303 for details on the 2X.)

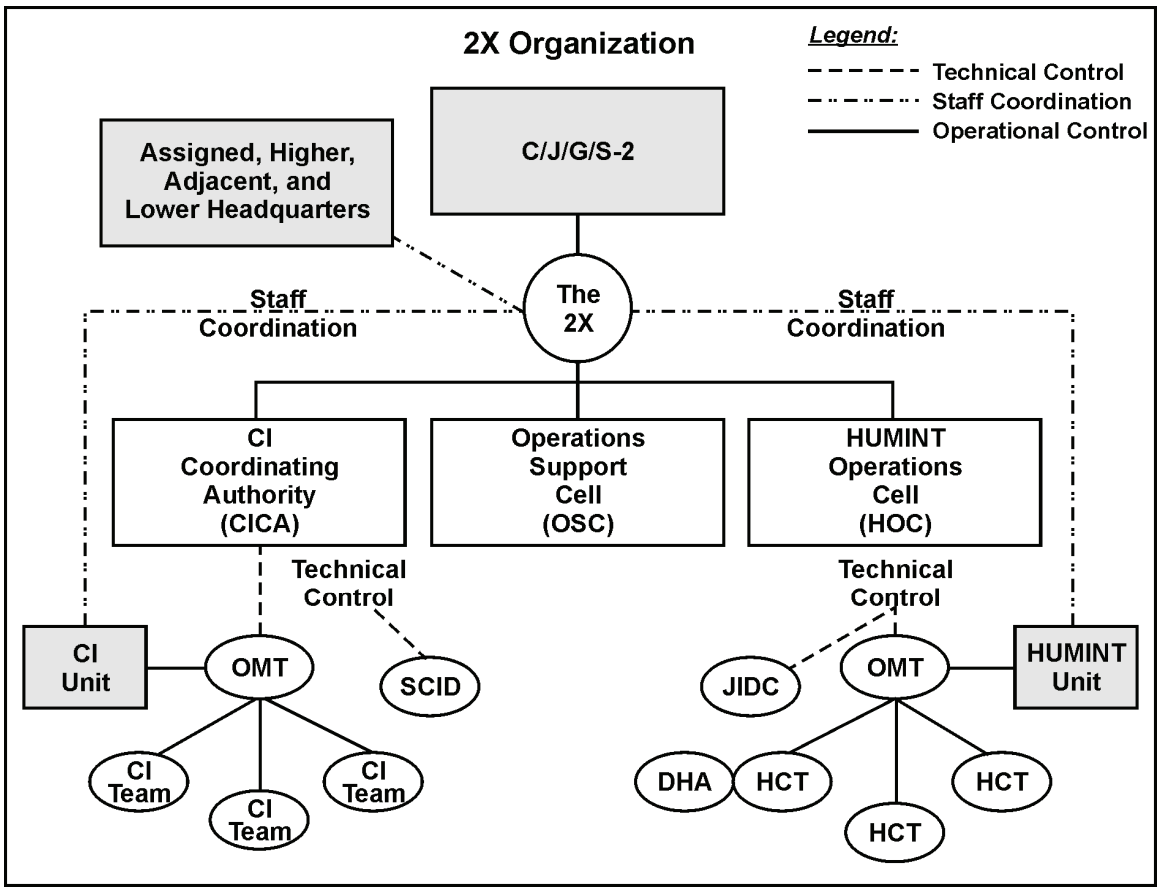

Figure 1-2. 2X organization

COUNTERINTELLIGENCE COORDINATING AUTHORITY

1-28. The CICA is the coordinating authority for all CI activities assigned or attached to Army CI assets within their unit or AOs. The CICA for Army divisions and corps will normally be a senior 351L CI WO. At the ASCC or theater level, the CICA may be a senior CI WO, CI officer (35E) or equivalent Military Intelligence Civilian Excepted Career Program (MICECP) government civilian employee.

1-29. Within joint and combined force commands, the TFCICA may be an Army, Navy, Air Force, or Marine Corps WO, officer, or civilian depending on the requirements of the approved joint manning document. Army CICA components are generally comprised of four personnel (a CI WO and three enlisted CI Soldiers); however, size and structure may vary depending on the unit and mission. Units engaged in operational and strategic missions may have a higher standard of grade for CICAs including the use of appropriately credentialed government civilian employees. CICA personnel may be attached, assigned, or under operational control (OPCON).

1-30. Regardless of echelon or Service component, the CICA's mission is to manage, coordinate, and synchronize all CI activities in the designated AO. The CICA exercises technical control over all CI entities and deconflicts CI activities with higher, lower, and adjacent CI elements. The CICA accomplishes all responsibilities through coordination with the operational units and other 2X staff elements. (See TC 2-22.303 for details on the CICA.) See table 1-1 (page 1-8) for the functions performed by CICA.

Table 1-1. Counterintelligence coordinating authority functions

CICA performs the following functions
• Coordinate and staff all CFSO proposals with the Army component or JTF approval authority, and U.S. national agency representatives. • Serve as the single focal point for all matters associated with CI in the area of intelligence responsibility. The CICA tracks CI activities and keeps the 2X informed, in turn the 2X keeps the C/J/G/S-2 and commander informed. • Exercise technical control of all CI entities and coordinate all CI activities in the area of intelligence responsibility. Coordinate with MI unit commanders who possess CI assets that execute CI activities in the AO. • Coordinate and deconflict all CI source operations with the source registry manager in the area of intelligence responsibility. • Ensure a robust CI education and awareness training program by coordinating CI refresher training, as required, and by ensuring the establishment of CI reporting channels and procedures in the area of intelligence responsibility. • Implement the intelligence program for all CI activities in the theater in accordance with AR 381-10.
Note. The MILDEPs always remain in control of CI investigations. The ATCICA and ACICA provide investigative technical control of all Army CI-conducted investigations. Army CI investigative reports pass through the CICA and 2X while simultaneously passing through the ATCICA and ACICA.
• Keep the 2X, C/J/G/S-2, and commander informed on the status of CI activities. • Coordinate with the analytical element and the ISR synchronization staff to identify and refine requirements for CI collection, operations, or investigations. • Ensure CI reporting is disseminated to the analytical element for inclusion in the all-source picture, as appropriate. • Develop and disseminate requirements, orders, and RFIs to CI entities in the area of intelligence responsibility. • Ensure registration of all CI sources with the OSC or other designated source registry manager. (If there is no OSC, the CICA will maintain the source registry.) • Routinely evaluate CI source operations to ensure proper handling by CI special agents, source ability to satisfy requirements, and to determine value of continuing the operation. • Ensure exploitation opportunities are preserved while conducting VAs and other protection initiatives. • Ensure investigations are planned, coordinated, and executed in accordance with applicable directives and regulations. • Establish and maintain connectivity with the supporting ATCICA for investigative oversight of Army CI-conducted investigations. • Participate in the operations staff targeting process to provide input on the placement, access, availability of sources, and reporting reliability of CI sources that support targeting. (For more information, see appendix B.) • Ensure CI support is provided to the JIDC and DHAs in the area of intelligence responsibility. • Establish quality control and execute release of all CI reporting. • Routinely provide feedback to all CI entities in the area of intelligence responsibility regarding collection activities, operations, and investigations. • After a determination has been made to release a detainee, ensure detainee screening is performed to determine the detainee's suitability as a potential lead for CI or other collection activities. • Interact with the HOC and OSC to ensure CI activities do not conflict with HUMINT activities in the area of intelligence responsibility. • Conduct liaison with the PMO and intelligence entities conducting liaison with HN LEAs to ensure CI activities are coordinated and deconflicted. • Conduct liaison with HN and U.S. national level CI organizations. • Provide staff oversight to LEPs screening activities within the area of intelligence responsibility. • Provide technical oversight and guidance for coordination or approval requests of CI operations that require approvals outside the local approval authority. • Recommend to the supported C/J/G/S-2 and maneuver commander the designation of an MI unit or intelligence staff element, as appropriate, to serve as the repository for CI badge and credentials in the area of intelligence responsibility. The MI unit or intelligence staff element should have responsibility for accountability and issue of CI badge and credentials. • Coordinate requests for CI technical services (cyber CI unit, TSCM, and polygraph support).

ACICA–Army CI coordinating authority	JTF–joint task force
AO–area of operations	LEA–law enforcement agency
ATCICA–Army theater CI coordinating authority	LEP–locally employed person
CI–counterintelligence	MI–military intelligence
CFSO–CI force protection source operations	MILDEP–military department
DHA–detainee holding area	OSC–operations support cell
HN–host nation	PMO–Provost Marshal Office
HOC–HUMINT operations cell	RFI–requests for information
ISR–intelligence, surveillance, and reconnaissance	TSCM–technical surveillance countermeasures
JIDC–Joint Interrogation and Debriefing Center	VA–vulnerability assessment

HUMAN INTELLIGENCE OPERATIONS CELL

1-31. The HOC is an element within the C/J/G/S-2X section that manages all HUMINT military source operations and related HUMINT activities, including debriefing, interrogation, screening, contact operations, and document and media exploitation (DOMEX) liaison. (See TC 2-22.303 for details on HOCs.)

OPERATIONS SUPPORT CELL

1-32. The OSC is an element within the C/J/G/S-2X section that manages overall 2X section operations, performs office administration functions, and accomplishes tasks that support both the CICA and HOC. The OSC serves as the operations officer and office manager for the 2X section. Each echelon with a 2X is also required to have an OSC. If the OSC is not authorized or resourced, the 2X determines how and by whom the OSC functions will be accomplished.

1-33. When the OSC is authorized or resourced, it works directly for the 2X. At lower echelons (for example, Stryker brigade combat team [SBCT] and brigade combat team [BCT] level), an OSC may not be authorized or resourced and may have to be task-organized to provide this capability. At higher echelons, an OSC is required given the span of control, the number of CI special agents and HUMINT collectors being managed, the amount of CI and HUMINT requirements, the large volume of reporting, and the increased burden of administrative requirements. (See TC 2-22.303 for details on the OSC.)

1-34. When established, the OSC requires intelligence personnel. Personnel qualified for an OSC assignment include all-source intelligence officers (35D), CI officers (35E), HUMINT officers (35F), CI technicians (351L), HUMINT technicians (351M), area intelligence technicians (351Y), HUMINT collectors (35M), CI special agents (35L), and Army, MICECP, and defense civilians. Civilians should be job series 0132, intelligence operations specialist (CI or HUMINT), or job series 0134, intelligence operations technician (CI or HUMINT). Qualified contractors can be assigned to an OSC in an appropriate supporting role such as a portal manager or in a reports officer position. The OSC handles common tasks and functions that support the CICA and HOC. See table 1-2 (page 1-10) for the functions performed by OSC.

Table 1-2. Operations support cell functions

OSC performs the following functions
• Provide 24-hour watch for the 2X section and serve as the central communications hub for the 2X section when deployed. Serve as the primary point of entry for all reporting from all outside echelons and elements. Maintain 2X section computer systems and communications equipment to ensure connectivity to CI and HUMINT entities in the area of intelligence responsibility. • Receive and track responses to all RFIs from all echelons. • Manage administrative support to the 2X section including in-and-out processing, tracking of efficiency reports and awards, and maintaining office files, as appropriate. • Coordinate logistic support and accounts for 2X section property. • Maintain a transmittal log for all requests and responses to and from external agencies, staffs, and authorities. • Coordinate movement of 2X section personnel with the C/J/G/S-3, dispatch and track 2X section vehicles, track and account for 2X section personnel in a travel status. • Serve as the 2X section's interface with the analytical element and ISR synchronization element. The OSC manages the intelligence cycle for the 2X section by receiving requirements and— ▪ Ensuring the requirements are clear. ▪ Advising the ISR synchronization element on the appropriateness of the received or forthcoming requirements. ▪ Helping to ensure that the best CI and HUMINT assets are tasked to satisfy the requirements. ▪ Ensuring that resulting reporting is appropriately disseminated to requestors. • Manage SDRs and release of IIRs. • Manage the intelligence property book, ICFs, and the Source Incentive Program.
Note. Army regulations require that separate individuals manage the ICF and Source Incentive Program, unless an exception is granted by the Army G-2.
• Maintain the consolidated source registry and reports databases, and assist the CICA and HOC in deconflicting MSO. • Coordinate with the linguist support section regarding linguist support to CI and HUMINT entities. • Coordinate with the C/J/G/S-2 operations section and C/J/G/S-3 regarding release of FRAGOs, as required.
CICA–CI coordinating authority FRAGO–fragmentary order HOC–HUMINT operations cell ICF–intelligence contingency fund IIR–intelligence information report ISR–intelligence, surveillance, and reconnaissance HUMINT–human intelligence MSO–military source operations OSC–operations support cell RFI–request for information SDR–source-directed requirement

Counterintelligence Operational Management Team

1-35. The OMT is the first operational management element that provides technical control and oversight to subordinate CI teams. The OMT manages subordinate CI teams to ensure operational execution and direction, quality and control of reporting, and satisfaction of intelligence requirements. An OMT can manage between one to four CI teams depending on the operational pace, mission, and geographic requirements. OMTs generally consist of four personnel (a 351L, CI WO and three 97L, CI enlisted Soldiers), but size and structure may vary depending on the unit and mission.

1-36. Units engaged in operational and strategic missions may also have a higher standard of grade for OMTs including the use of appropriately credentialed government civilian employees. OMT personnel may be attached, assigned, or under OPCON. OMTs and subordinate CI teams may be assigned or attached from higher echelon units to lower echelon units. Depending on mission requirements, CI OMTs may be held at the next higher echelon of the subordinate CI teams. CI OMTs will not normally be located below the brigade level. (See TC 2-22.303 for details on the OMT.) See table 1-3 for the functions performed by OMT.

Table 1-3. Operational management team functions

OMT performs the following functions
• Disseminate all intelligence or time-sensitive information to the supported or responsible command channels for action or operational consideration. • Provide guidance and technical control to operational activity. • Provide collection and operational focuses for CI teams. • Provide quality control and report dissemination to subordinate CI teams.

Table 1-3. Operational management team functions (continued)

OMT performs the following functions
• Receive, edit, and provide feedback on all administrative reports, such as readiness status and operational reports, and on intelligence reports, such as IIRs, submitted by subordinate teams. • Ensure CI reporting and related traffic is fused into all-source intelligence. • Conduct CI analysis and assist in mission analysis for the supported commander. • Coordinate CI activities with the CICA and with CI element commanders in the area of intelligence responsibility. • Perform liaison with HN and U.S. national level security, intelligence, and law enforcement organizations. • Inform respective CICA when Army CI elements are conducting CI investigative activities within the purview of AR 381-20. • Act as a conduit between subordinate CI teams, the CICA, and 2X, and the supported unit headquarters. • Provide administrative support to subordinate CI teams, including reporting mission and equipment status to the CICA or HOC and the supported unit headquarters. • Educate the supported commander on the subordinate teams' capabilities. • Integrate subordinate CI teams directly into the maneuver commander's ISR planning.
AR–Army regulation CICA–CI coordinating authority HOC–HUMINT operations cell IIR–intelligence information report ISR–intelligence, surveillance, and reconnaissance HN–host nation

Counterintelligence Team

1-37. The CI team conducts CI investigations, CI collection (debriefings, source operations, liaison, and screening), CI analysis, and CI technical services support to protect the supported unit from threat intelligence activities.

1-38. The CI team provides the supported commander, through 2X channels, a capability to help protect the force and affect the adversaries' understanding of friendly force operational capabilities. The CI team also provides capabilities to help answer CCIRs and SCICRs related to FISS and ITO collection activities targeted against the supported unit, Army, and DOD equities.

1-39. A CI team generally consists of four 35L, CI noncommissioned officers (NCOs), and enlisted Soldiers. Units engaged in operational and strategic missions may also have a higher standard of grade for CI teams including the use of appropriately credentialed government civilian employees. Specialized CI teams, including technical counterintelligence (TCI), cyber CI, and polygraph teams, may vary in size and composition (2- to 3-person military or civilian teams) based on mission requirements and unit organization. CI teams—

- May be attached, assigned, or under OPCON.
- May be attached or assigned from higher echelon units to lower echelon units.
- Are typically assigned at division and above levels; however, they may be attached or assigned at brigade level depending upon mission requirements.

1-40. Table 1-4 (page 1-12) lists the functions performed by the CI team.

Table 1-4. Counterintelligence team functions

OSC performs the following functions
• Prepare and submit command reports, such as readiness status reports that provide status of equipment, personnel, and ICF in accordance with supporting OMT SOPs. • Prepare protected reports, such as contact reports, in accordance with OMT SOPs, that document each source contact. ▪ Disseminate contact reports to supporting OMT for review or comment. ▪ Maintain contact report files on every source. ▪ Provide contact report files to relief team during relief in place or transfer of authority. • Prepare and submit intelligence reports, such as spot reports, using the SALUTE format, and IIRs in accordance with OMT SOPs. • Assist in the production of threat and vulnerability assessments. This function provides support to evaluations of installations and operating bases with MP, CA, engineers, and medical units to identify the intelligence threat to the operating location. The VA identifies weaknesses in operational and physical security procedures and recommends countermeasures to mitigate intelligence collection on friendly forces, limiting the ability of adversaries to plan and conduct hostile acts against U.S. and multinational activities and locations. • Conduct CI analysis to support mission requirements and contribute to the all-source common operational picture. To verify adequate area coverage, use backwards planning and source profiling to choose CI targets. Develop and use CI target overlays and other CI analytical tools that illustrate the CI situation, identify CI gaps, and help refocus CI collection efforts. • Conduct CI debriefings. This function involves the systematic questioning—using direct and indirect questioning techniques—of individuals to procure information that answers specific CI collection requirements. Sources for debriefing include friendly forces (for example, MP, CA, engineers, and medical units), U.S. and non-U.S. civilians including members of NGOs, refugees, displaced persons, and local inhabitants. The CI team regularly and systematically debriefs all ISR assets. • Conduct CI investigations within the jurisdictional boundaries of Army CI regulations and the guidelines of AR 381-10, AR 381-12 and AR 381-20. Regularly coordinate with the supporting staff judge advocate to ensure investigations are conducted to support eventual trial and prosecution, if necessary, and in compliance with all DOD policy and U.S. laws. • Conduct CI screenings. CI screenings serve two purposes: ▪ Collect information of CI interest or to collect established information requirements through the interview of indigenous, third-country nationals, foreign expatriates, or U.S. military personnel in the AO. ▪ Interview and assess the suitability and security risks of employing potential candidates with U.S. forces to support LEP screening programs at installations and forward operating bases. • Conduct CI collection. This function includes activities focused on identifying adversary intelligence threats that target U.S. and multinational interests. CI collection is conducted through use of sources and other multimedia sources to obtain information that impacts the supported unit. CI collection activities will not be used as a substitute for Army HUMINT collection. “Collect” specific information or develop leads that can obtain information concerning adversary intelligence collection requirements, adversary capabilities, adversary personalities, and adversary methods of operation targeting U.S. and multinational forces. • Register all CI contacts through the OMT and CICA in the source registry. Disseminate CI administrative, technical, and intelligence reports through the OMT and CICA. • Conduct CI liaison with U.S., multinational, and host-nation military and civilian agencies, including NGOs, for the purpose of obtaining information of CI interest and to coordinate and deconflict CI activities. Liaison activities are designed to ensure a cooperative operating environment for CI elements and to develop CI leads for further exploitation. ▪ Maintain constant contact with the supported S-2 to identify intelligence requirements, information gaps, and to deconflict operations within the support commander’s AOs. ▪ Maintain constant contact with other ISR assets (scouts, PSYOP, CA, and MP) to coordinate and deconflict operations in adjacent AOs and cross-checks collected information. • Support the CI Education and Awareness Training Program by coordinating with the S-2 to present CI awareness training to all units in the area of intelligence responsibility. CI teams should be the focal point for all CI training to identify incidents of CI interest and educate Army personnel about their responsibilities to report incidents outlined in AR 381-12. The CI Education and Awareness Training Program supports the commander’s overall protection program. • Provide CI technical service support, such as polygraph, TSCM, computer forensics, to the supported unit when properly trained and equipped personnel are available.

AO–area of operations	MP–military police
CA–civil affairs	HUMINT–human intelligence
CI–counterintelligence	NGO–nongovernmental organization
CICA–CI coordinating authority	OMT–operational management team
DOD–Department of Defense	PSYOP–psychological operations
ICF–intelligence contingency fund	SALUTE–size, activity, location, unit, time, equipment
IIR–intelligence information report	SOP–standing operating procedure
ISR–intelligence, surveillance, and reconnaissance	TSCM–technical surveillance countermeasures
	VA–vulnerability assessment

U.S. AND DEPARTMENT OF DEFENSE COUNTERINTELLIGENCE COMMUNITY

1-41. Each of the following organizations serve the U.S. and DOD intelligence community, specifically in CI matters:

- Office of the National Counterintelligence Executive (ONCIX).
- Federal Bureau of Investigation (FBI).
- Central Intelligence Agency (CIA).
- Deputy Under Secretary for Defense (DUSD), Counterintelligence and Security (CI&S).
- Defense CI and HUMINT Center.
- Counterintelligence staff officer (CISO).

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE

1-42. The ONCIX is subordinate to the Office of the Director of National Intelligence (DNI). The ONCIX serves as the U.S. Government executive agent for all CI matters and is responsible for developing the CI strategy for the U.S. CI community including DOD CI elements. The ONCIX advises the DNI on CI program budgets and evaluations to ensure the CI community is properly funded to execute operations that support national policy and strategic priorities. The ONCIX establishes priorities for CI collection, investigations, and operations to—

- Exploit and defeat FISS and ITO collection activities directed against U.S. interests.
- Protect and sustain U.S. intelligence systems and agencies.
- Neutralize and exploit adversarial intelligence activities targeting the armed forces.

FEDERAL BUREAU OF INVESTIGATION

1-43. The FBI is the investigative arm of the Department of Justice and is a member of the intelligence community under the provisions of Title 50, USC The FBI is the lead U.S. Government agency for CI within the United States. Army CI often conducts joint CI investigations with the FBI when the offense or the subject falls within the investigative jurisdiction of Army CI.

CENTRAL INTELLIGENCE AGENCY

1-44. The CIA is the lead U.S. Government agency responsible for foreign intelligence and CI activities outside the United States. However, most CIA CI activities are focused on protecting the integrity and security of CIA operations from compromise. Army CI collection and operations outside the United States must be deconflicted with the CIA to avoid intelligence conflicts and ensure unity of the intelligence effort.

DEPUTY UNDER SECRETARY FOR DEFENSE, COUNTERINTELLIGENCE AND SECURITY

1-45. The DUSD (CI&S) is responsible for providing oversight of the DOD CI Program and making recommendations on policy issues to the DUSD for intelligence. DUSD (CI&S) serves as the OSD staff focal point for all issues relating to DOD CI initiatives. DUSD (CI&S) also interacts with other DOD staff elements, the National Counterintelligence Executive and other national agencies to help direct and shape CI strategies.

DEFENSE COUNTERINTELLIGENCE AND HUMAN INTELLIGENCE CENTER

1-46. In August 2008, the DOD simultaneously disestablished the CI Field Activity and activated the Defense CI and HUMINT Center, which is under the direction of the Defense Intelligence Agency (DIA).

The new center has no law enforcement function. It manages CI programs for DOD and integrates overlapping CI and HUMINT operational and support areas.

COUNTERINTELLIGENCE STAFF OFFICER

1-47. The CISO serves as an advisor on CI matters to the combatant command J-2 and commander. The CISO assists in providing oversight on all the command's CI activities and ensuring all command plans and operational planning include CI operations, requirements, and tasking when appropriate. The CISO also provides management and deconfliction of CI collection, production, investigations, operations, and technical services capabilities within their theater or area of responsibility.

1-48. The CISO establishes combatant command CI priority intelligence requirements (PIRs) to support the commander's information requirements. When a combatant command is designated as a joint task force (JTF) command headquarters, the CISO can serve as the TFCICA until joint manning documentation establishes a recurring requirement to fill that position for the duration of the operation. CISOs may also be documented in ASCC staffs as required and authorized.

ARMY COUNTERINTELLIGENCE LEVELS OF EMPLOYMENT

1-49. CI is critical to Army operations at all echelons, across the spectrum of conflict. Army CI can and will execute all five CI core competency functions from the tactical to strategic operational environments. The only difference in the operational execution is generally what mission areas are being supported. Even CI special agents providing CI technical services and support are leveraged to provide their unique capabilities during stable peace and during major combat operations.

1-50. All Army commanders, including commanders of MI units, need to be educated by senior CI and HUMINT personnel to clearly define the distinctions between the two disciplines to ensure the effective use of both disciplines to support the unit's mission. Since CI personnel have been used instead as HUMINT collectors during the past 15 years, senior CI special agents have failed to articulate the CI's true mission to their commanders and how proper employment of CI is a warfighting enabler. This failure to articulate—combined with a lack of HUMINT resources and an increased reliance on human-derived information as a catalyst for military operations execution—has blurred the identity of CI, especially at the tactical level.

STRATEGIC AND DEPARTMENTAL CI

1-51. Strategic operations are conducted by CI elements supporting national and DOD missions (for example, support to North Atlantic Treaty Organization [NATO] and special operations and missions). Strategic CI also conducts compartmented investigations and operations to affect the knowledge of FISS and ITO regarding contingency operations and defense information. Strategic CI executes the full range of CI functions and missions including CI investigations and operations, offensive counterintelligence operations, RTP, special access program support, treaty verification, and technical CI services (polygraph, TSCM, and computer forensics). Strategic CI also supports special operations forces and special mission units within the scope of applicable national, DOD, and DA policies and regulations. Strategic and departmental CI assets generally conduct the following activities:

- **Advice and assistance—**assist unit security managers and commanders with knowledge on security programs and provide details on reporting potential FISS and ITO targeting and incidents of CI interest.
- **Education and awareness—**provide FISS and ITO threat and Army program briefings to educate unit personnel, satisfy mandatory training requirements, and generate potential leads for incidents of CI interest.
- **Threat assessments (TAs) and vulnerability assessments (VAs)—**conduct collection and analysis of FISS and ITO threat data for a specific unit, facility, operation or activity to

provide the supported commander knowledge on protection and security posture and make countermeasures recommendations to overcome deficiencies.

- **CI investigations—**exploit or neutralize potential FISS and ITO collection threats targeting Army and DOD equities.
- **CI collection—**detect and identify FISS and ITO intelligence collection activities targeting U.S. forces and to devise other CI initiatives to counter, exploit, or neutralize the FISS and ITO collection capability.

Army G-2X

1-52. At the departmental level, the Army G-2X is the executive agent for all Army CI activities including policy implementation, operational oversight, intelligence funding programs, and Army staff level management. It coordinates with other military Service and national agency intelligence and CI services to coordinate CI strategies and mutually supporting activities, including joint CI operations and investigations. The Army G-2X is responsible for making recommendations to the DA G-2 concerning all budgetary issues concerning CI and HUMINT.

1-53. The Army G-2X provides oversight and guidance to Army CI elements. It staffs and coordinates approval of CI operational concepts and plans, as outlined in AR 381-20, to ensure they meet legal sufficiency satisfy validated requirements. The Army G-2X also provides oversight of all approved Army CI operational concepts and plans. It manages and maintains the Army's centralized CI and HUMINT source registry and product library, as part of a joint Service CI and HUMINT database. The Army G-2X coordinates functional and technical support services, as well as comprehensive worldwide FISS and ITO threat analysis products. The Army G-2X collaborates with theater and maneuver CI staff and field elements to ensure unity of the CI effort and efficient use and employment of Army CI assets.

Army Counterintelligence Coordinating Authority

1-54. The ACICA is subordinate to the Army G-2X and is responsible for implementing and enforcing U.S. and DOD policy within the Army and providing oversight and technical control of all Army CI activities. The ACICA reviews, staffs, and coordinates all special investigative and collection techniques requested by Army CI elements. ACICA is responsible for approving all Army CI investigations, and for reviewing, staffing, and coordinating all CI operational plans and concepts with the appropriate agencies and approval authorities. It coordinates with other U.S. Government and military CI agencies to assist in the development and implementation of national CI strategies.

Intelligence and Security Command

1-55. The Army Intelligence and Security Command (INSCOM) executes departmental and operational CI activities with guidance from the Army G-2X. INSCOM has the responsibility for administrative C2 of all MI brigades supporting their respective theaters. INSCOM CI assets are task-organized and operationally employed based on mission and geographic requirements. Most MI brigades organize their CI assets into detachments with subordinate field or resident offices.

OPERATIONAL

1-56. Operational level CI assets are generally assigned to ASCC or combatant command organizations and are focused on a specific theater. CI, at the operational level, is primarily focused on CE and CI support to protection. Operational CI assets are instrumental in protecting bases of operations from infiltration, collection, planning, and targeting by FISS and ITO entities. Although operational CI elements have a vital mission to counter the FISS and ITO threat on a daily basis, they may be tasked to deploy and support contingency or combat operations. This is especially true in large-scale combat operations when the size, scale, and scope of the operation exceeds the capability of organic tactical CI assets to provide adequate support in the AO. When required, operational CI assets may be tasked to support strategic CI operations. Operational CI assets generally conduct the following activities:

- **Advice and assistance—**assist unit security managers and commander's with knowledge on security programs and provide details on reporting potential FISS and ITO targeting and incidents of CI interest.
- **Education and awareness—**provide FISS and ITO threat and CI awareness briefings to educate unit personnel, satisfy mandatory training requirements, and generate potential leads for incidents of CI interest.
- **TAs and VAs—**conduct collection and analysis of FISS and ITO threat data for a specific unit, facility, operation, or activity to provide the supported commander knowledge on protection and security posture and make countermeasures recommendations to overcome deficiencies.
- **CI screening—**vet locally employed persons (LEPs) in overseas and deployed locations for suitability to work, protection liabilities, associations, or contacts that may allow them to be used in other CI collection initiatives.
- **CI investigations—**exploit or neutralize potential FISS and ITO collection threats targeting Army and DOD equities.
- **CI collection—**detect and identify FISS and ITO intelligence collection activities targeting U.S. forces and devise other CI initiatives to counter, exploit, or neutralize the FISS and ITO collection capability.

Theater Army G-2X

1-57. The theater Army G-2X is the principal advisor to the theater Army G-2 and commander for all CI and HUMINT matters. The theater Army G-2X consists of the G-2X staff officer, theater HOC, Army theater counterintelligence coordinating authority (ATCICA), and OSC. It provides guidance and oversight based upon Army G-2X directives and theater requirements. It provides technical control, operational coordination, and CI oversight of all theater Army CI and HUMINT elements. The theater Army G-2X also coordinates technical support services, source registration and national level product support with the Army G-2X. Regional analysis and production is provided to theater consumers and forwarded to the Army G-2X for inclusion into the national database.

Army Theater Counterintelligence Coordinating Authority

1-58. The ATCICA is subordinate to the theater G-2X and is responsible for providing direct oversight, guidance, and technical control of all Army CI collection, investigative, and operational activities within their theaters of operations, including CI elements assigned to tactical organizations. ATCICA is responsible for reviewing and staffing all requests for special investigative and collection techniques and investigative and operational plans and concepts. The ATCICA is the interface between subordinate Army CI operational management elements and the ACICA. It is responsible for implementing Army CI policy as directed by the ACICA and Army G-2X. It conducts liaison with other U.S. Government, military, and host-nation (HN) intelligence, security, and law enforcement agencies (LEAs) to coordinate and deconflict CI activities.

Military Intelligence Brigade

1-59. MI brigades provide operational support to the separate ASCCs. CI elements in MI brigades support combatant commanders. Operational level CI activities and functions include: investigations, collection, analysis and production, and technical services and support. CI elements must be capable of quickly transitioning from a peacetime mission to crisis operations to support combatant commander requirements. Theater CI assets conduct Army, joint, and multinational operations in designated theaters. Operational elements may also be deployed to support or reinforce operating forces.

TACTICAL

1-60. Tactical level CI generally denotes all CI assets assigned to Army division and below echelons (BCTs, and divisions). CI at the tactical level is primarily focused on CI support to protection to their supported commander's during operations. CI assets at the tactical level are instrumental in protecting bases of operations from infiltration, collection, planning, and targeting by FISS and ITO entities.

1-61. Tactical level CI assets generally do not have a robust peacetime mission since their focus is providing support to their Army forces parent organization; however, in some cases, operational and strategic CI elements may formally request their support on a case-by-case basis or through formal written agreements. Even during peacetime, garrison operations tactical CI assets are essential in providing advice and assistance to their supported command. Depending on the size, scale, and scope of ongoing operations, operational and strategic CI assets may also be tasked to augment tactical operations. CI assets assigned to tactical units generally conduct the following activities:

- **Advice and assistance—**assist unit security managers and commanders with knowledge on security programs and provide details on those CI assets that can respond to FISS and ITO targeting.
- **Education and awareness—**provide FISS and ITO threat and CI awareness briefings to educate unit personnel, satisfy mandatory training requirements, and generate potential leads for CI elements chartered to conduct investigations during peacetime.
- **TAs and VAs—**conduct collection and analysis of FISS and ITO threat data for a specific unit, facility, operation, or activity to provide the supported commander knowledge on protection and security posture and make countermeasures recommendations to overcome deficiencies.
- **CI screening—**vet LEPs in overseas and deployed locations for suitability to work, protection liabilities, associations, or contacts that may allow them to be used in other CI collection initiatives.
- **CI investigations—**identify potential CI investigation requirements and triage those incidents for other CI assets chartered to conduct the investigation. This can be accomplished during peacetime and contingency or combat operations. During contingency or combat operations, the chartered CI element may request the assistance of tactical CI personnel to fulfill investigative requirements. Tactical CI assets generally do not have the resources to effectively execute a complex CI or CE investigation.
- **CI collection—**detect and identify FISS and ITO intelligence collection activities targeting U.S. forces and to devise other CI initiatives to counter or neutralize the FISS and ITO collection capability. CI collection is only conducted in contingency or combat operational environments and when approved by the CICA.

CORPS/DIVISION/BRIGADE G-2X

1-62. The G/S-2X is the principal advisor to the supported commander for all CI and HUMINT matters within the AO. The G/S-2X consists of the G/S-2X staff officer, HOC, and the CICA. At lower echelons (for example, SBCT and BCT level), an OSC may not be authorized or resourced and may have to be task-organized to provide this capability.

1-63. The G/S-2X provides direct technical control and oversight to all CI and HUMINT assets within the unit and area of intelligence responsibility. The G/S-2X—

- Coordinates and deconflicts all CI and HUMINT activities between higher, lower, and adjacent 2X elements.
- Is responsible for providing and maintaining a consolidated source registration for all CI and HUMINT elements within the area of intelligence responsibility and providing source data to the next higher echelon 2X element.
- Coordinates requests for technical support services, source registration, and higher level analytical support with the next higher echelon 2X element.
- Must have knowledge of CI and HUMINT resources and capabilities for all military, DIA, and U.S. Government agencies. The G-2X must be able to transition from an Army force operation to functioning as a J-2X if the unit is designated as a JTF headquarters.

Corps/Division Counterintelligence Coordinating Activity

1-64. The corps/division CICAs are directly subordinate to their respective corps/division G-2X element. The CICA provides direct oversight and control for all CI activities within the supported unit and area of intelligence responsibility. The CICA is responsible for coordinating and deconflicting all CI activities with next higher echelon CICA. It conducts liaison with other U.S. Government, military, and HN intelligence, security, and LEAs within their area of intelligence responsibility to coordinate and deconflict CI activities. The CICA—

- Reviews and provides quality control and dissemination of all CI reporting from subordinate CI elements.
- Provides operational analysis to focus CI activities, assess responsiveness and effectiveness of CI activities, and ensures coverage of information requirements for their supported commander.
- Must have knowledge of the CI resources and capabilities of all military, DIA, and U.S. Government agencies.
- Must be able to transition from an Army force operation to functioning as a TFCICA if the unit is designated as a JTF headquarters.

Corps/Division Counterintelligence Elements

1-65. CI assets supporting division and JTF operations are generally leveraged from battlefield surveillance brigades (BFSBs). The G-2X at division will provide CI investigation and operational oversight along with technical control of CI elements supporting division elements. The division G-2X will coordinate CI activities through the JTF J-2X in theater and the theater CICA and senior CISO. The division G-2X is trained and equipped to act as a J-2X if the division is designated as the JTF command element during a contingency operation. At corps/division level, the BFSB MI battalion has three companies with CI assets. The C&E company has one CI OMT that controls three CI teams. Each CI team consists of four enlisted CI Soldiers. The C&E company's mission is to provide general support coverage for the division. Each of the two CI and HUMINT companies has two CI teams and no CI OMT. The CI and HUMINT company's mission is to provide its assets in direct support to the BCTs.

Brigade Combat Team

1-66. Within a BCT are no organic CI OMTs or CI teams in the MI company. CI support assigned or attached to the BCT includes an OMT or is controlled by the BCT S-2X/CICA. CI teams assigned or attached to the BCT conduct operations in a direct support role throughout the BCT's AO.

Chapter 2

Counterintelligence Investigations

Counterintelligence (CI) investigations are conducted to detect, identify, assess, counter, neutralize, or exploit the foreign intelligence and security services (FISS) and international terrorist organizations (ITO) threat to the Army and Department of Defense (DOD). The first priority for all CI investigative situations is to assess for possible exploitation. Offensive exploitation of situations or persons involved wittingly or unwittingly in providing information to a FISS and ITO entity provides the best long-term solution for controlling damage to national security, fully exploiting or understanding the threat to Army and DOD equities, and degrading the adversarial collection activity. If a situation or person cannot be controlled to the advantage of Army CI, neutralization of the threat through exposure or prosecutorial measures will be pursued.

INVESTIGATIVE PERSONNEL

2-1. CI investigations are conducted only by CI personnel who have been trained and certified by the Army Intelligence Center and Fort Huachuca (USAIC&FH). Additionally, only those CI personnel assigned or attached to units with a CI investigative mission are authorized to conduct a preliminary inquiry (PI) or a full field investigation (FFI). Personnel authorized to conduct CI investigations are commissioned officers who possess area of concentration (AOC) 35E; warrant officers (WOs) who possess AOC 351L; enlisted military occupational specialty (MOS) personnel who possess MOS 35L and have been issued badge and credentials; or by Army civilian employees in career field 0132, who are assigned to CI units, have been school-trained, and are issued badge and credentials. (See AR 381-20 for more information on training and badge and credentials requirements.)

2-2. Local national and contract investigators employed by overseas Army CI units that have been issued military intelligence (MI) representative credentials may support the investigative effort through analysis, research, and by obtaining documentation. They will not be primary or sole investigators on any investigation.

2-3. Contractors are not authorized to perform CI investigations and operations. They are authorized to support CI activities that include conducting CI analysis, forensic examinations and analysis, translations and interpretations, CI database maintenance, CI awareness briefings, CI threat assessments (TAs), vulnerability assessments (VAs), and CI screenings of contract linguists.

COUNTERINTELLIGENCE INVESTIGATION OBJECTIVES

2-4. CI investigations are essential to counter threat collection efforts targeting Army equities. CI places emphasis on investigative activity to support force and technology protection, homeland defense, information assurance, and security programs. CI investigations focus on resolving allegations of known or suspected acts that may constitute national security crimes under U.S. law or the Uniform Code of Military Justice (UCMJ).

2-5. The initial objective of CI investigations is to identify people, organizations, and other entities engaging in national security crimes and to determine the full nature and extent of damage to national security. The intent is to develop information of sufficient value to permit its use in the appropriate civil or military court. However, investigations should not be limited to the production of evidence. Investigative reports should include all relevant information as it pertains to the person or incident involved in the investigation. CI investigations are conducted to—

- Identify people, organizations, and other entities engaging in national security crimes that impact Army equities.
- Determine the full nature of national security crimes within the authority and jurisdiction of Army CI.
- Prove or disprove allegations or indications that person or persons are engaged in national security crimes or incidents of CI interest.
- Prevent the loss, control, or compromise of sensitive or classified defense information and technology.
- Protect the security of Army personnel, information, operations, installations, and technology.
- Acquire and preserve evidence used to support exploitation, prosecution, or any other legal proceedings or punitive measures resulting from CI investigations.
- Detect and identify terrorist activities that may present a threat to Army, DOD, and national security.

2-6. CI investigations must conform to applicable U.S. laws and DOD and DA regulations. CI special agents must report information accurately and completely. They maintain files and records to allow transfer of an investigation without loss of control or efficiency. Coordination with other CI or law enforcement organizations ensures that investigations are conducted as rapidly as possible. It also reduces duplication and assists in resolving conflicts when jurisdictional lines are unclear or overlap. CI investigative activity must be discreet, ensuring the rights and privacy of individuals involved, as well as the preservation of all investigative prerogatives. This is required to protect the rights of individuals and to preserve the security of investigative techniques.

2-7. CI special agents need to have a thorough understanding of all investigative techniques and planning, approval processes, and legal requirements before requesting and initiating any type of CI investigative activity. A lack of understanding in any one of these areas may potentially invalidate any investigation from a prosecutorial standard and may jeopardize the ability to exploit a threat to the United States.

INVESTIGATIVE AUTHORITY

2-8. DODI 5240.04 and AR 381-20 are the source documents for policy on the conduct of CI investigations in DOD and Army, respectively. In addition, the Delimitations Agreement of 1979 establishes jurisdictional boundaries and operational procedures that govern the conduct of CI activities by the DOD CI organizations in conjunction with the Federal Bureau of Investigation (FBI).

2-9. SIA represents the investigative acts an agent conducts without the Army CI coordinating authority (ACICA) opening an investigation. It allows the CI special agent to gather enough information to provide a detailed CI incident report concerning all incidents within the purview of CI investigative authority. This allows adjudication by the ACICA or the responsible Army theater CI coordinating authority (ATCICA) to determine whether further investigative activities are required or a CI incident report is submitted to the ATCICA. SIA is not to be used to circumvent case control mechanisms or to expedite cases.

2-10. CI SIA includes—

- Interviewing the source or best sources or other persons knowledgeable of the suspected incident to establish facts of the incident, fully identify subjects, identify all associated persons, and additional investigative leads.
- The conduct of records checks including local agency checks (LACs) and military agency checks (MACs), Army personnel and unit records, and local intelligence files to fully identify the subject or subjects of the incident.
- Collection and retention of physical evidence not requiring approval under the provisions of AR 381-10.
- CI debriefing of returned special category absentees, defectors, detainees, and repatriated prisoners of war (POWs) in the special agent's AO immediately upon notification.
- Monitoring command inquiries for incidents that may be of CI interest.

Note. Under no circumstances will the subject or potential subject be interviewed without prior approval from ATCICA or ACICA.

COUNTERINTELLIGENCE INVESTIGATIVE JURISDICTION

2-11. In accordance with EO 12333, DODD 5240.1-R and 5240.2, and AR 381-20, Army CI has investigative authority concerning criminal statutes under USC Title 18 and corresponding criminal articles in the UCMJ or incidents of CI interest, if the subject or potential subject meets the CI investigative jurisdiction. Army CI has primary jurisdiction, concurrent jurisdiction, or joint jurisdiction in investigative matters under the provisions of AR 381-20.

PRIMARY AUTHORITY

2-12. Army CI has investigative primacy for the national security crimes and incidents of CI interest listed below when they are committed by persons identified as subjects. If either the subject, potential subject, incident, or crime falls outside Army CI jurisdiction, Army CI may still retain joint investigative responsibilities.

- Sedition.
- Aiding the enemy by providing intelligence to the enemy.
- Spying.
- Espionage.
- Subversion.
- Treason.
- Terrorism activities or materiel support to a known or suspected terrorist organization or person (DCS G-2, G-2 Memorandum (S//NF), 24 August 2005).
- Incidents of CI interest.

Note. Under no circumstances will the subject or potential subject be interviewed without prior approval of the ACICA.

CONCURRENT AUTHORITY

2-13. CI investigating elements will coordinate with other agencies to ensure efficient exchange of investigative information when the element discovers information that may also fall under the investigative purview or jurisdiction of another agency. Army CI will concurrently investigate the following incidents when a CI interest has been established:

- Sabotage.
- Incidents of CI interest.

JOINT AUTHORITY

2-14. Army CI may seek joint investigative authority with the agreement of the other military or civilian law enforcement agencies (LEAs) and the ATCICA or ACICA for—

- National security crimes involving other DOD affiliated individuals when Army equities exist.
- Incidents of CI interest.

SUBJECTS

2-15. Inside the United States, Army CI is responsible for investigations of active duty U.S. military personnel. The FBI is responsible for investigations of all civilian personnel, private DOD contractors, and their employees. Army CI has primary investigative jurisdiction for retired personnel, active and inactive Reservists, and National Guard members when the act or acts under investigation occurred while the individual was on Active Duty status.

2-16. Outside the United States, Army CI has investigative jurisdiction over active duty military personnel and their family members, current and former DOD civilian employees and their family members, current and former foreign national employees and their family members, and DOD contractors and their family members, subject to coordination with the FBI, CIA, or host government agencies; retired military personnel; Army Reserve personnel; members of the National Guard while in the performance of DOD duties; and foreign nationals who are applicants for DOD employment.

INCIDENTS OF COUNTERINTELLIGENCE INTEREST

2-17. The following is not an all-inclusive list of incidents of CI interest:

- The activities of ITO or material support to an ITO or person. Terrorist organizations are specified in DCS, G-2 Memorandum (S//NF), dated 13 February 2007, Operational Planning List (OPL) 2005 (U), as revised.
- Unreported contact with foreign government personnel, persons or groups involved in foreign terrorism or intelligence, or unauthorized requests for classified or sensitive unclassified information.
- Unauthorized disclosure of classified information or material. Not all incidents in this category may meet the threshold for a CI investigation. However, those that do will often include other indicators of espionage that are identified associated with the incident or when there are acts which are known methods of operations of FISS and ITO entities. Investigations are conducted to ascertain those entities involvement. CI special agents may also act to secure classified material and to determine if the actions of the subject were an act of omission or commission. The command requirements to report compromises or conduct inquiries as specified in AR 380-5, chapter VI, may also apply to these incidents.
- Matters developed as a result of counterintelligence scope polygraph (CSP) examination as specified in AR 381-20.

- Military personnel or DAC employees who perform unofficial travel to those countries designated in the operational planning list, who have unauthorized contact with official representatives of foreign countries, or who contact or visit foreign diplomatic facilities without authorization.
- Attempts by authorized users of information systems to gain unauthorized access.
- Known, suspected or attempted intrusions into classified or unclassified information systems when there is reasonable suspicion of foreign involvement or it has not been ruled out.
- Unauthorized removal of classified material or possession of classified material in unauthorized locations.
- Special category absentees (SCAs), which include those absent without leave (AWOL), deserters defectors, and military absentees who have had access to TS, SCI, SAP information, or TS cryptographic access or an assignment to a special mission unit within the year preceding the absence. CI special agents will conduct investigations of the circumstances surrounding the absences of SCA personnel using the guidelines presented in this manual.
- Army military, civilian, or overseas contractor personnel declared AWOL and deserters who had access within the preceding year to TS, SCI, critical military technology as defined in AR 381-20, chapter 7, SAPs; personnel who were assigned to a special mission unit; personnel in the DA Cryptographic Access Program (DACAP); and personnel with access to critical nuclear weapons design technology.
- Army military, civilian, or overseas contractor personnel who go absent without authority, AWOL, or deserters who do not have assignments or access; however, there are indications of FISS and ITO contact or involvement in their absence.
- DA military and civilian personnel who defect and those persons who are absent without authorization and travel to or through a foreign country other than the one in which they were stationed or assigned.
- DA military and civilian personnel detained or captured by a government, group, or adversary with interests inimical to those of the United States. Such personnel will be debriefed upon return to U.S. control.
- Attempted or actual suicide or suspicious death of a DA member if they have an intelligence background, were assigned to an SMU, or had access to classified information within the year preceding the incident, or where there are indications of FISS and ITO involvement.
- Suspected or actual unauthorized acquisition or illegal diversion of military critical technology, research and development information, or information concerning an Army acquisition program. If required, Army CI will ensure all appropriate military and civilian intelligence and LEAs are notified. Army CI will also ensure Army equities are articulated and either monitor the status of the agency with primary jurisdiction or coordinate for joint investigative authority.
- Impersonation of intelligence personnel or unlawful possession or use of Army intelligence identification, such as badge and credentials.
- Communications security (COMSEC) insecurities, except those which are administrative in nature. (See AR 380-40, chapter 7.)
- Suspected electronic intrusions or eavesdropping devices in secure areas which could be used for technical surveillance. DA personnel discovering such a device will not disturb it or discuss the discovery in the area where the device is located.
- Willful compromise of clandestine intelligence personnel and CI activities.

COUNTERINTELLIGENCE INVESTIGATIVE CONTROL AND OVERSIGHT

2-18. The Deputy Chief of Staff, G-2 (DCS G-2), exercises DA staff oversight and technical authority for all CI activities and is responsible for appointing Army G-2X. The Army G-2X is the Army's executive agent for all Army CI activities at the Army staff level. On behalf of the DCS G-2, the Army G-2X formulates policies for the conduct, management, direction, and control of CI investigations.

2-19. For the Army G-2, the Army G-2X maintains the ACICA who provides daily technical management, control and oversight for all Army CI functions, including, investigations, collection, operations, projects, programs, collection, reporting and analysis. The ACICA exercises technical control and coordination for all Army CI elements and is the ultimate case control over all investigations.

2-20. The ACICA exercises technical control, review, coordination, and oversight of Army CI controlled activities. The ACICA has specific responsibility to—

- Act as the ultimate approval authority to open or initiate and close or terminate CI investigations.
- Assign case control numbers for tracking and operations security (OPSEC) purposes.
- Serve as the single focal point for all CI investigative referrals to or operational coordination with national intelligence, CI, and LEAs, Office of Personnel Management (OPM).
- Provide CI expertise to outside continental United States (OCONUS) ASCCs in the establishment of ATCICA when directed.
- Refer information which is not under Army CI investigative jurisdiction and which does not involve Army equities to appropriate security, intelligence, or LEAs.
- Review of CI investigative and operational reports for quality assurance and intelligence oversight.
- Coordinate for review of legal sufficiency.
- Ensure that closed, completed, or terminated case files, project files, source dossiers records, and reports are properly classified or declassified and retired to the U.S. Army Investigative Records Repository (USAIRR).
- In coordination with appropriate ATCICA, review information derived from active and terminated CI investigations to ensure any information meeting intelligence reporting requirements is properly submitted using IIR format.
- Maintain a database for all Army CI investigations.

2-21. The ATCICA is responsible for providing the ASCC with the technical expertise to ensure that CI activities are conducted in a competent, legal, and proper manner within their AOR. The ATCICA will perform the following functions:

- Serve as the central focal point for monitoring the conduct of CI controlled activities within an AOR.
- Assignment of case control numbers to CI preliminary inquiries for tracking and OPSEC purposes.
- Coordinate with the ACICA opening and closing CI investigations, and be responsive to requirements of and direction from ACICA.
- Provide theater-wide technical management, control, and oversight of all Army CI activities, including investigations. This includes activities conducted by non-INSCOM CI units and elements operating in a deployed status in the ATCICA AOR.

- Act as the principal Army interface with the theater joint or combatant commander on all CI activities.
- Provide action or information copies to ACICA on all CI investigative reporting, including CI incident reports, investigative plans (IPs), and requests for approval for special investigative techniques in accordance with AR 381-10.
- Task investigative elements within theater and pass lateral leads to other ATCICA elements, with an information copy to the ACICA.
- Ensure all 381-10 procedural requests are reviewed by the command legal officer or SJA and intelligence officer before being forwarded to approval officials.

2-22. Commanders of units with a CI investigative mission are responsible for ensuring that the ACICA has full knowledge of all CI investigations. The commander has responsibility to—

- Ensure all CI units and personnel submit all CI reporting to the ATCICA and respond to tasking from the ATCICA and ACICA using the most direct channel.
- Ensure the ATCICA is informed of all significant CI investigations and operations so that the ATCICA and ACICA are properly prepared to inform or brief the chain of command.

COUNTERINTELLIGENCE INVESTIGATION TYPES AND CATEGORIES

2-23. CI investigations focus on a person, incident, or systemic issue that are of potential interest to CI. The subject and type of incident identified during the initial reporting of a CI matter will often determine the type of investigation required as well as the scope of the investigation, resources, and various types of investigative techniques required to effectively investigate and resolve the incident. Investigations generally begin as incident investigations concerning acts or activities which are committed by, or involve, known or unknown persons or groups. The amount of information obtained during lead development concerning persons involved and the threat posed to Army equities will determine the type of investigation that will be conducted.

LIMITED COUNTERINTELLIGENCE ASSESSMENT

2-24. Army CI investigative elements conduct investigative activity under limited CI assessment (LCA) in response to information which normally does not require the submission of a CI incident report in accordance with AR 381-12, paragraphs 3-1, 3-2 and 3-3, but which still represents a potential CI threat to the Army and DOD. LCA investigative objectives are to quickly collect available information through relatively nonintrusive means to clarify and establish CI interest, or to effectively determine that no CI threat information exists. Army CI investigative elements may engage in the following investigative activities under LCA, consistent with their assigned CI investigative mission:

- Collect publicly available information, as well as information from online services and resources available to and as approved for use by the reporting CI element.
- Conduct records checks with military units and offices, including Army personnel and finance centers, for example:
  - Checks with other federal, state, and local law enforcement and intelligence organizations.
  - Checks with HN law enforcement and intelligence organizations OCONUS.
  - Reviews Army CI and Army intelligence files and databases.
- Collect and retain items for evaluation as physical evidence not requiring approval under the provisions of AR 381-10.

- Interview previously established Army CI sources and liaison contacts. This does not allow for the new tasking of those recruited assets.
- Accept information voluntarily provided by any military, government, or private persons or entities. Army CI special agents may always accept and review voluntarily provided information or materials to determine potential CI interest.
- Interview or request information (other than under pretext) from Army affiliated persons and members of the public and private entities. Interviews or RFIs from non-Army affiliated personnel or entities are authorized, subject to existing coordination requirements with other agencies or authorities, such as the FBI in the continental United States (CONUS), and CIA chiefs of station and HN authorities OCONUS in accordance with an existing Status of Forces Agreement (SOFA). In areas without a SOFA or in contingency areas, local commanders will provide appropriate guidance. Interviews of investigative subjects, potential subjects, or any other persons which would require a rights warning are not authorized during investigative activities associated with LCA.
- Provide assistance to inquiries of supported commands conducted in accordance with AR 380-5 and AR 15-6 when related to matters of possible CI interest. Army CI investigative assistance to support such command inquiries will be limited to those activities identified above, and may be conducted in coordination with the appropriate commander or investigating officer. Additionally, Army CI special agents may participate in AR 380-5 and AR 15-6 investigative interviews only upon request by the command investigating officer. Army CI may not provide any assistance to investigating officers to support AR 380-5 and AR 15-6 investigations when no indication of possible CI interest exists, except as identified in AR 381-20. Army CI investigative personnel will ensure command investigative representatives fully understand that Army CI investigative assistance is conducted under authority of Army CI and not the command. AR 381-20 currently authorizes Army CI personnel to provide investigative advice to command security investigations.

2-25. Investigative activity under LCA is authorized for 60 days upon written approval by an Army CI special agent at or above the grade of O3/CW3/GG13 who occupies the position of commander, leader, or operations officer of an Army CI detachment, resident office, region, or other field element of an INSCOM major subordinate command (MSC) or the 650th MI Group. LCA approvals will be forwarded within 3 days for informational purposes to the INSCOM MSC/650th MI Group headquarters. Army CI special agents in possession of CI badge and credentials who are not assigned to INSCOM MSC/650th MI Group elements may conduct LCA investigative activities only upon written approval from the covering ATCICA or the ACICA.

2-26. In support of contingency deployments, the ATCICA or ACICA may grant temporary LCA approval authority to CI special agents at the grade of O3/CW3/GG13 or above, who are assigned to leadership or staff positions in non-INSCOM MSC/650th MI Group elements. LCA investigations will not exceed 60 days, unless specifically approved by the ATCICA, ACICA or an INSCOM MSC/650th MI Group commander based on written justification for the continued LCA investigative activity. Once terminated, results of LCA activity will be reported to respective INSCOM MSC/650th MI Group headquarters or the covering ATCICA by means of an executive summary or information paper which will include, at a minimum, the initial case predication, a summary of investigative results, and the reason for termination.

2-27. Investigative activities conducted under LCA will be documented within five work days via a memorandum for record (MFR) using locally assigned case control numbers and maintained in a standard investigative case file. Investigative reporting under LCA will not normally be archived in the USAIRR unless specifically required by the ACICA, ATCICA, or the INSCOM MSC/650th MI Group commander. If the matter progresses to a preliminary or full investigation, all investigative reporting under the LCA will be incorporated into the main preliminary or full investigative case file. At a minimum, investigative reporting under LCA will be maintained in accordance with the requirements under the Army Records Information Management System (ARIMS).

2-28. All activities conducted under LCA are subject to provisions of AR 381-10 regarding the collection, retention, and dissemination of U.S. person information, and will be regularly inspected under organizational inspection programs regarding their scope, management, and execution. All Army CI investigative elements will report statistics on a quarterly basis to their respective INSCOM MSC/650th MI Group headquarters or covering ATCICA concerning the number of LCA's initiated and terminated during the reporting period.

2-29. Army CI investigative elements will not utilize LCA as the basis for delaying or not submitting a CI incident report or local threat report as required by AR 381-12. After submission of a CI incident report, investigative elements will await case determination by the ACICA, ATCICA, or INSCOM MSC/650th MI Group headquarters before continuing investigative activity. If no preliminary or full investigation is opened as the result of a CI incident report, investigative elements have the authority to continue LCA activities to clarify or expand on information of possible CI interest.

PRELIMINARY INQUIRIES

2-30. A PI is a limited scope inquiry concerning reported incidents of CI interest to ascertain if a threat to national security exists; or a criminal offense within Army CI authority has occurred and warrants further CI investigative actions or resources. A PI can be locally approved by the CI investigating unit's responsible ATCICA after the submission of an CI incident report has been submitted. PIs may include the conduct of all investigative activities under SIA as well as the following:

- Interviews of sources other than the subjects or potential subjects to identify the subject.
- Regional, state, or HN records checks and National Crime Information Center (NCIC) queries.
- ACICA approval—pretext or subject interviews.
- When timing is critical and the action is approved by an official specified by AR 381-10, chapter 9, emergency surveillance may be conducted to identify a known or suspected agent, or official of foreign power or known or suspected member of a terrorist group. (See AR 381-20.)

2-31. PIs will be conducted at the direction of the responsible ATCICA. The ACICA, with the responsible ATCICA, will decide dispositions of all PIs. Disposition may include the following:

- Continuance or extension of PI.
- Transition to an FFI.
- Transfer of investigative interest to another investigative agency based upon priority of authority or investigative responsibility.
- Closure of the investigation if it is determined that no matters of CI interest are involved.

2-32. A PI must either be closed or transitioned to an FFI within six months, unless an extension is approved by the ACICA. If a reported incident or allegation has sufficient merit upon CI incident reporting, a PI need not be conducted as a precursor to the approval of an FFI.

FULL FIELD COUNTERINTELLIGENCE INVESTIGATIONS

2-33. FFIs are conducted when specific facts have been identified that someone under Army CI authority has committed or allegedly committed a national security crime or incident of CI interest.

2-34. An FFI may be initiated with the concurrence of the ACICA after the submission of a CI incident report.

2-35. The ATCICA is responsible for monitoring all investigative activities of opened FFIs within their AOR and to coordinate all requests for all special investigative techniques with appropriate approving

authority within AR 381-10 and to consult with the ACICA concerning the status and investigative activity for all FFIs within their AOR.

2-36. The ACICA may designate an FFI as a high priority based upon the significance of the investigation and threat to Army equities involved. Commander's of CI units who have an open FFI that has been designated as high priority by the ACICA will ensure that the FFI takes precedence over all other CI functions and will allocate appropriate levels of resources, manpower, and effort to the FFI.

SPECIAL CATEGORY ABSENTEE INVESTIGATIONS

2-37. SCA are personnel considered AWOL, deserters, defectors, and military absentees who are of potential interest to CI. CI investigative focus in SCA investigations is to determine if any national defense information was compromised or the offense was conducted at the direction or with the support of a foreign government, military, or intelligence agency or a known terrorist entity. Army CI SCA investigations are conducted to determine the following:

- Circumstances and motivation of the absence.
- Evidence of foreign intelligence or terrorist involvement or indications of potential espionage or subversion at the behest of a foreign entity.
- Indications of loss or compromise of classified or national defense information.
- Indications of or potential for defection or travel to or through a foreign country.
- Any connections in or with persons in foreign countries, including relatives.
- Depending upon the SCA status, AWOL, deserter or defector, refer to this manual for specific debriefing criteria.

2-38. Primary investigative jurisdiction for Army personnel declared AWOL rests with the Provost Marshal. Should the military member be declared a deserter, the U.S. Army Criminal Investigations Command (USACIC) assumes primary jurisdiction. Although Army CI does not have primary jurisdiction in SCA cases, Army CI may investigate for the reasons under CI investigative control and oversight.

2-39. When a CI element is notified of the absence of an SCA meeting, a CI incident report, citing the SCA as the subject, will be submitted within 72 hours to the responsible ATCICA. If the subject is not immediately returned to U.S. military control, the ACICA will make a determination to designate the case OPEN or TERMINATED.

2-40. CI elements need to establish a close working relationship with all PMOs, MP, and criminal investigation units within their AOR to ensure that these units are aware of the topics of potential CI interest that should be referred to CI.

INVESTIGATIVE PROCESS

2-41. The CI investigation process consists of lead development, planning and approval, investigative activities, and termination or transfer. See figure 2-1 for the investigative life cycle.

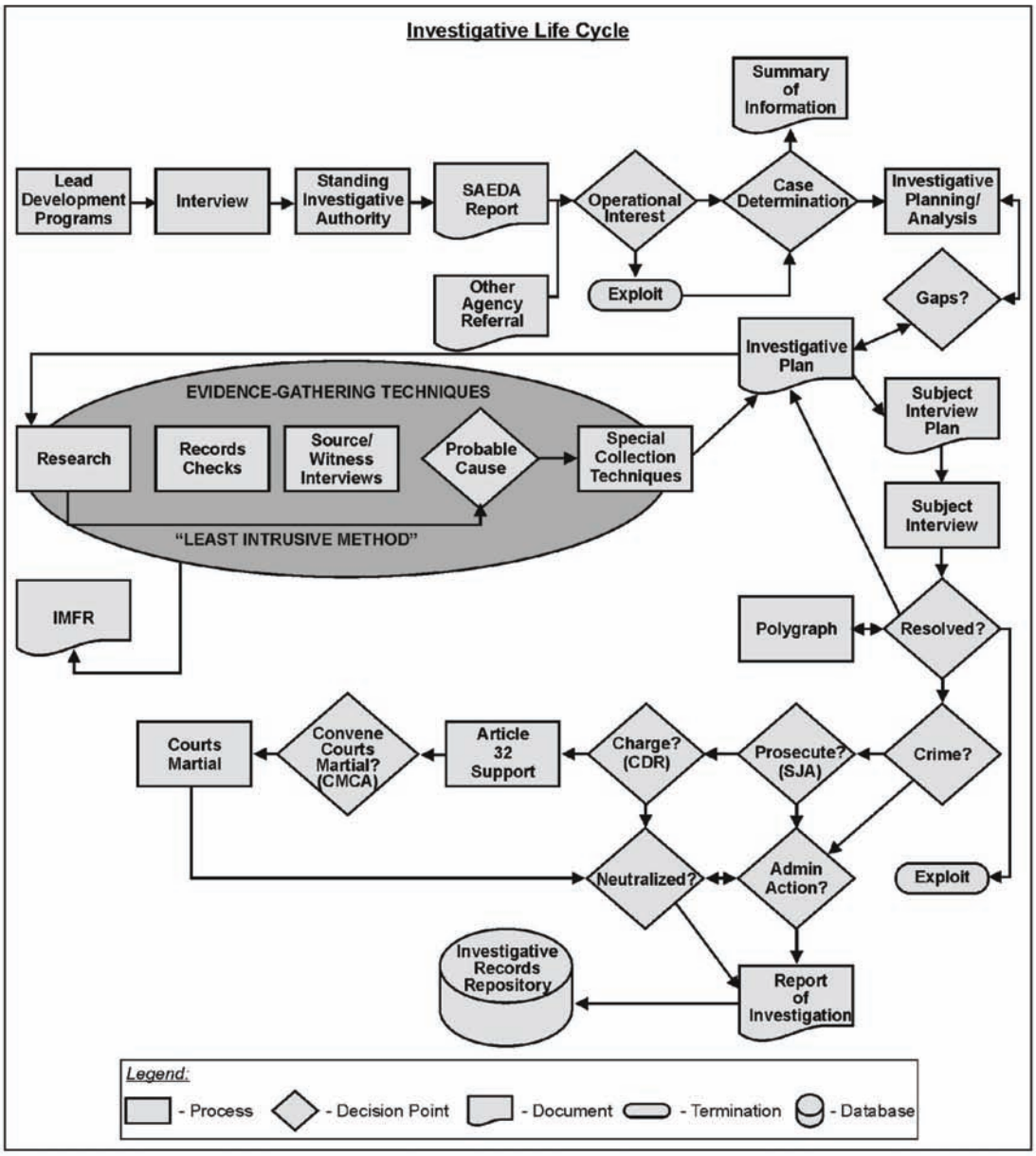

Figure 2-1. Investigative life cycle

LEAD DEVELOPMENT

2-42. A proactive CI program at all echelons, tactical to strategic, is required to educate military members (Soldiers, civilians, and contractors) and generate CI leads. Military members often do not understand what types of incidents are of interest to CI and may also not understand their reporting obligations under the provisions of AR 381-12. All five functions of CI (investigations, operations, collection, analysis, and technical services) can be used to identify and generate potential CI investigative leads.

2-43. A proactive CI program should, at a minimum, consist of an aggressive education and awareness program, close and professional relationship with supported commanding officers and unit security managers or officers. In addition to generating potential CI investigative leads, these activities can also support CI collection activities to answer SCICRs or unit CCIRs.

THE COUNTERINTELLIGENCE AWARENESS AND REPORTING PROGRAM

2-44. The CI Awareness and Reporting Program is an education, awareness, and reporting program to help identify potential incidents of CI interest. The program is a primary factor in obtaining information that is the basis for initiating CI investigations in response to suspected national security crimes under Army CI jurisdiction. AR 381-12 requires Army personnel, both civilian and military, to report matters of potential interest to CI. This program also mandates CI awareness training be scheduled by all units on an annual basis with the supporting CI office. CI training of personnel assigned to all units is subject to inspection by the Inspector General (IG) office as well as under the Command Inspection Program. CI awareness briefings should be given by qualified CI special agents whenever possible. CI awareness presentations should, at a minimum, contain—

- FISS and ITO collection methods of operation.
- Criminal penalties for the various national security crimes under CI authority.
- Type of situations and CI incidents of additional matters of CI interest that should be reported (see AR 381-12, chapter 3).
- Indicators of espionage (see figure 2-2).
- Reporting procedures, responsible CI elements, and the 1800 CALL SPY program.
- Initial Reporting.

2-45. The CI Awareness and Reporting Program, along with persons who have good situational awareness of CI reporting requirements, will generally be the initial source for identifying indicators or anomalies for incidents under the purview of CI authority.

Note. When operationally feasible, all CI incidents will be reported by the investigating CI special agent within 72 hours after receipt of the information. If the reported information identifies an imminent threat to U.S. forces, then the information needs to be reported immediately through command channels with a follow-up report provided to the ACICA or ATCICA.

2-46. All initial reports will be reported directly to the ACICA and a courtesy copy provided simultaneously to the responsible ATCICA and the chain of command (if the investigating agent belongs to an operational CI unit). If the investigating CI special agent is unsure whether the reported incident meets the criteria of those reportable matters specified in AR 381.12, a report will be submitted to the ACICA and ATCICA for a determination. The investigating CI special agent will obtain as much information as possible from the initial source including—

- Pertinent details of the suspected incident, date, time, time span, locations, suspected acts, conversational details, information involved.
- Personal information concerning known additional sources of the reported incident, witnesses to the incident or subjects or potential subjects involved in the incident. A person is considered known when they can be identified by at least a first and last name and unit of assignment or employment location).
- Physical descriptions of unidentified witnesses to the incident or subjects or potential subjects involved in the incident.
- Personal information concerning the source of the information.

PLANNING AND APPROVAL

2-47. Due to the legal complexities involved in CI investigations, investigative planning and approval has to be detailed and meticulous to maintain the legal integrity of the case and/or to compartmentalize the

knowledge of the incident to allow for potential exploitation of the incident. The ACICA will review and approve all IPs and subject interview plans (SIPs) submitted by the investigating element.

Indicators of Espionage

- Any attempt to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities or attempting to obtain information for which the person has no authorized access or need to know.
- Unauthorized removal of classified materials from work area or unauthorized possession of classified materials outside the work areas, such as in residences or vehicles.
- Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified material which may exceed job requirements.
- Repeated or unrequired work outside normal duty hours, especially unaccompanied.
- Obtaining witness signatures on classified document destruction forms when the witness did not observe the destruction.
- Bringing unauthorized cameras, recording devices, computers, or modems into areas where classified data is stored, discussed, or processed.
- Unexplained or undue affluence, including sudden purchases of high-value items (real estate, stocks, vehicles, or vacations, for example) where no logical income source exists. Attempts to explain wealth by reference to inheritance, luck in gambling, or some successful business venture.
- Opening several bank accounts containing substantial sums of money where no logical income source exists.
- Free spending or lavish display of wealth which appears beyond normal income.
- Sudden reversal of financial situation or sudden repayment of large debts or loans.
- Correspondence with persons in countries listed in AR 381-12.
- Unreported contact with officials of countries listed in AR 381-12.
- Frequent or unexplained trips of short duration to foreign countries.
- Attempts to offer extra income from an outside endeavor to personnel with sensitive jobs or to entice them into criminal situations which could lead to blackmail.
- Homesteading or repeatedly requesting extensions to tours of duty in one assignment or location, especially when the assignment offers significant access to sensitive information or the job is not desirable.
- Repeated involvement in security violations.
- Joking or bragging about working for a foreign intelligence service.
- Visits to a foreign embassy, consulate, trade, or press office.

Figure 2-2. Indicators of espionage

2-48. If the ACICA determines that a CI incident report merits CI investigation, it will direct that one be initiated and, except for full field CI investigations, the responsible ATCICA will maintain technical control, management, and oversight of all investigative activities within their AOR. All investigative reporting, plans, and requests for special investigative techniques will be forwarded to the ATCICA for review and quality control before submission to the ACICA for higher levels of approval or before forwarding to the approving authority. Interagency investigative coordination will be the responsibility of the CI element on the ground. If problems with interagency cooperation arise, they will be forwarded to the appropriate element commander to raise the issue to the appropriate agency headquarters.

Investigative Plan

2-49. The IP is the document that provides a detailed road map on the conduct of CI investigations including all investigative participants, all investigative activities required, all resources and external support required, and all interagency or legal coordination required to successfully resolve the incident. IPs are living documents and may require revision due to information development and case direction. All updates or revisions will be forwarded to and approved by the ACICA before implementation.

2-50. An IP is required in all open FFIs for investigative actions. IPs are not usually required for a PI; however, the responsible ATCICA may direct the submission of an IP based upon the circumstances of the PI. An IP is prepared by the lead agent in collaboration with the senior supervisory CI special agent and the ATCICA. The IP is used to outline and request approval for investigative authority; however, some investigative activities may require submission of additional documentation for coordination and approval. The submission date for the IP will be directed by the responsible ATCICA and unit SOPs. Note that in especially sensitive or high visibility cases IP approval may rest with a higher headquarters, ASCC, ACICA, or Headquarters, DA (HQDA) level. While the format for IPs may vary slightly between all the ATCICAs, the content of the IP will, at a minimum, include the following:

- **References.** The subject block or title for the CI incident report and any subsequent investigative reports that precipitated the opening of the investigation by the ACICA.
- **Title.** The subject block with the assigned Army case control number assigned by the ACICA in the investigation opening message.
- **Background.** A synopsis of the incident under investigation.
- **Investigative objectives.** Identification of subjects and relationships between subjects and FISS and ITO; confirming, mitigating, or refuting the suspected allegations concerning the subjects; the nature and/or extent of the compromise of classified information or technology; to assess the damage to national security; determine the involvement and methodologies of FISS and ITO.
- **Investigative actions.** All projected activities required to conduct the investigation and resolve the incident including records checks (local and military), interviews of all persons who may be able to provide details concerning the incident, all persons who may be considered witnesses to the incident and subjects interviews, any projected approvals for interviews, general or investigative techniques, submission of final report of investigation (ROI).
- **Joint investigative coordination.** All activities conducted with or supported by external military, civilian, or HN agencies during the course of the investigation.
- **ICF.** The projected amount of funds required to support all investigative activities through the life of the investigation.
- **Coordination required.** All activities by external agencies required to support the investigation which may include technical support for special investigative techniques; legal coordination before subjects interview; coordination for apprehension, detention, and searches by the appropriate approval authority.

Updating Investigative Plans

2-51. An IP will be updated when there is a change in focus of the investigation, or a major occurrence that sheds new light on the evidence or shows a new direction for the investigation to follow. To avoid confusion and errors in communications, there can be only one IP as the sole investigative guide for planned or projected investigative activity in the affected case. Therefore, an updated IP must supersede all previous versions. The lead agent and the desk officer must assume that, in the natural course of an investigation, developed facts and information will dictate a revision to the IP. A revised IP can be written at any time. It is not necessary to wait for the ATCICA or ACICA to update IP. At or near the transition from one phase to another, the entire case should be reviewed to ensure it remains focused, the investigative activity supports the objectives and follow-on activities are appropriate. It is not necessary to finish every investigative action in the original approved IP before submitting an updated IP or to finish all investigative actions in the original IP before starting the investigative actions requested and approved in the updated IP.

Joint Investigative Plans

2-52. IPs are required for the Army CI portion of joint investigations. Investigative planning in joint investigations can be problematic. Other military and other government agencies (OGAs) do not have the same organizational culture or administrative requirements as Army CI. In some cases their planning process is more diffuse and approval levels are much lower. Early and frequent coordination is the key to avoiding misunderstandings and miscommunication. This is critical in joint investigations where Army CI is not the lead agency.

2-53. IPs in joint investigations will be prepared in the normal format and provided to the supervisory agent for the lead agency for coordination and concurrence. In cases in which Army CI participates in a joint investigation with another agency, it will document the action with a written agreement between the parties. In either case it will be reflected in the IP forwarded to the ATCICA for approval with the name of the lead agency official and date of concurrence. Field agents should be aware that coordination and discussion may occur at multiple headquarters levels on their investigations. The joint IP is the foundation of common understanding regarding the investigation and is the basis for all coordination at higher levels.

Subject Interview Plan

2-54. Once the ACICA has directed or granted approval for a subject interview of a CI investigation, the CI element will develop a SIP. The purposes of the SIP are—to ensure the agent is familiar with all information obtained during the course of the investigation and clearly understands the goals of the subject interview; serves as a mechanism to identify and coordinate outside support as required; serves as approval to actually schedule and conduct the subject interview, and may serve as the vehicle for legal review of the subject interview proposal.

2-55. It is not required including specific questions in the SIP; however, depending on the complexity of the issues to be discussed this can often be helpful. At a minimum, before conducting the interview the agent should develop a topical outline that can be used to ensure all subject interview objectives and requirements are met. If it is likely that a polygraph examination will follow the subject interview, the polygraph detachment should review the case file and suggest questions for inclusion in the SIP to ensure an effective polygraph. The ATCICA, or a CI supervisor with the delegated authority, will approve all SIP in writing, before their execution. The SIP will include the following:

- **Title.** The subject block with the assigned Army case control number assigned by the ACICA in the investigation opening message.
- **Background.** A synopsis of the incident under investigation.
- **Investigation objectives.** Lists all the goals of the subject interview including—

  - Obtaining information to confirm, mitigate, or refute, for example, the possibility the subject promised to provide, caused to be provided, and/or provided restricted U.S. defense information to unauthorized personnel in an unauthorized manner.
  - Identifying the subject's affiliation with any other foreign entity; that subject deliberately compromised or willfully disclosed classified U.S. defense information.
  - Ascertaining that the subject engaged in any national security crime. Investigative objectives also include identifying FISS and ITO methods of operation and the extent of damage caused to national security.
- **Results of the investigation to date.** A brief synopsis of all investigative activities and the corresponding results preceding the subject interview.
- **Purpose of the interview.** Identification of all persons involved in the suspected allegations; the extent of compromise; all the details concerning the suspected allegations; assessment for potential exploitation.
- **Administrative information**. Include all participants in the subject interview, date, location and whether or not the interview will be audio or video recorded.
- **Conduct of the interview.** Include introductions, identification, rights warning or waiver and other administrative procedures, topical areas of the interview or, if required by the ATCICA, a line of questioning; closure of the interview including assessment on subject disposition (released, released to his chain of command or detention or apprehension by appropriate authorities).
- **Coordination required.** Any type of external CI coordination required to support the interview including the SJA for legal advice on charges; MP for possible custody assumption; any joint participants (for example, Army CID or FBI).
- **Lead agent.** Name, title, and contact information for the investigating agent conducting the interview.

Requesting Special Investigative Techniques

2-56. All requests for the below listed special investigative techniques will be submitted through the ATCICA to the ACICA for coordination and approval by the appropriate authority. AR 381-10 provides detailed guidance on the separate approval authorities for all special investigative techniques both in the United States and abroad. The IP may discuss the potential use of special investigative techniques, but will not be used as the vehicle to document, coordinate, and approve these techniques.

Note. No special investigative techniques will be conducted unless coordinated by the ACICA and approved by the responsible authority.

2-57. When considering the use of a special investigative technique to support a CI investigation, the least intrusive means of achieving the goals of the investigation must be the primary consideration. If a more intrusive special investigative technique is used other than one that would or could reasonably achieve the same investigative result, the legal integrity of the CI investigation may be subject to challenge or dismissal during potential criminal proceedings. The following special investigative techniques are used to support CI investigations:

- Procedure 5—Electronic Surveillance.
- Procedure 6—Concealed Monitoring.
- Procedure 7—Physical Searches.
- Procedure 8—Mail Searches and Examination.

- Procedure 9—Physical Surveillance.
- Procedure 10—Undisclosed Participation.

Staff Judge Advocate Coordination

2-58. While the primary objective in all established CI investigations is exploitation, if the situation does not allow for Army CI to control the situation, then the threat has to be neutralized. In cases where prosecution is a possibility, CI investigative personnel should consult with the SJA throughout the investigation, after coordination with the ACICA and obtaining command approval. Continuous legal consultation during the investigation will support the prosecution's case and provide insight to the investigating CI special agent regarding case direction. SJA can assist the CI investigative process by—

- Providing legal advice for unique situations, such as offenses rarely charged or pursued.
- Helping to clarify or resolve multiagency jurisdiction disputes and questions.
- Assisting with identifying specific criminal offenses for individual cases.
- Coordinating with the CI special agent to discuss interview legalities, rights warning waivers, and hostile interview courses of action (COAs).
- Assisting with the legal coordination and approval for apprehension, detention, and search warrants with prior coordination and approval of the ACICA.
- Preparing criminal proceedings.
- Providing intelligence oversight review for proposed CI activities.
- Providing advice and assistance in the preparation of proposals for special investigative techniques.

2-59. All CI investigations will be conducted to a prosecutorial standard in accordance with applicable U.S. laws and DA and DOD regulations. CI investigations of national security crimes must produce findings which are accurate, concise, and legally sufficient for admission into a court of military or civil law. Investigations must be conducted in accordance with the principles of law and the rules of evidence which govern the prosecution of any criminal activity. AR 195-5 and FM 3-19.13 cover the legal aspects of gathering, handling, documenting, and controlling evidence. CI personnel must have a thorough understanding of the legal principles and procedures involved in conducting an investigation for three reasons:

- To strictly apply them in all investigative activity.
- To ensure prosecutorial integrity even during emergency circumstances that does not permit the opportunity to seek legal guidance before exercising investigative authority.
- To provide the CI special agent an experience base to recognize those cases where specific guidance, assistance, and/or approval must be obtained before executing any further investigative activities.

2-60. Basic legal principles will always apply to CI investigative situations. Legal principles are designed to ensure that the legal rights of subjects or suspects are observed. It is important to ensure that the potential ability to prosecute any given case is not jeopardized by illegal or improper CI investigative techniques. In addition, CI personnel involved in investigative activities must obtain advice and assistance from the SJA or legal officer to implement recent court decisions interpreting statutes and regulations.

INVESTIGATIVE ACTIVITIES

2-61. All investigations will vary in scope, objective, and resources to successfully resolve the incident under investigation. The IP is the primary planning tool to spur a logical thought process to identify all the various types of investigative activities that should be considered to conduct the investigation. Investigative

activities should be tailored to each investigation. Investigative activities should be sequenced to ensure a swift and successful completion of the investigation. The following are those general investigative activities that will be common to most CI investigations.

- Files and records checks for pertinent information.
- Individual interviews for additional information and leads.
- Exploitation of new leads and consolidation of all available data for analysis and planning a COA.
- Interview of the subject to prove or disprove the allegations.
- Requests for assistance (RFAs) for CI support or investigative activities from other law enforcement, security, or intelligence agencies.

2-62. Detailed planning is the key to preserving OPSEC and preventing the premature disclosure of the investigation. The OPSEC objective is to ensure that the subject not be aware that anything is going on until the subject interview; otherwise, the subject will likely change his patterns or habits that could disrupt the investigation and potentially destroy any evidence required for prosecution.

2-63. While preparing the IP, the least intrusive method for obtaining information concerning the incident or subject should always be the primary consideration. The least intrusive method will be the one which allows the CI special agent to obtain the necessary information to prove or disprove the allegations against the subject, while obtaining the necessary probable cause needed to justify more intrusive collection techniques. IPs are progressive, and more intrusive investigative techniques may be required based upon the complexity and legal sufficiency needed to support the investigation and any follow-on legal proceedings. Investigative activities addressed in the IP should consider the following:

- Sequence investigative activity from least to most visible. The closer the investigation gets to the subject the higher the risk to jeopardizing the legal credibility of the investigation.
- Use less visible, less intrusive techniques to establish the subject's social network and patterns. Detailed knowledge of how the subject lives day-to-day life is critical to OPSEC planning.
- Carefully identify "best sources" for required information and approach the fewest people possible to develop critical information. There is always time to interview additional witnesses after subject becomes aware.
- Be cognizant of how much information you are giving away as you collect evidence. Do not reveal specific accusations or details to witnesses. When conducting records checks, consider asking for information about the subject's entire section or unit vice solely focusing on the subject.
- Remember that your presence alone can reveal your interest.
- Consider the use of ruses and cover stories. A survey can sometimes be used to develop general information about the subject's workplace and work habits.
- When making inquiries or conducting interviews the CI special agent should refrain from using threatening terms such as espionage or terrorism. For example, the CI special agent should address the investigation as an inquiry into an incident of CI interest, security matter, or violation. This will usually gain more cooperation from witnesses or persons with knowledge of the subject or incident being investigated.
- Always have a backup plan if the subject discovers your investigative interest. Examples: What would change? Would simultaneous interviews of friends and co-workers now be appropriate? How about an early subject interview? Do you want to conduct searches before the subject can hide or destroy evidence? Is the subject likely to flee? Do you have enough evidence and do you know how to have the subject detained if necessary.

Media Inquiries

2-64. Be prepared for inquiries by local, national, or foreign media. In some cases subjects themselves will contact local media in an effort to undermine an investigation. Under no circumstances will CI special agents respond to media inquiries without the consent and approval of the responsible ACICA. The standard response to such requests will be to refer the caller to INSCOM or other appropriate Public Affairs Office (PAO), followed by immediate telephonic notification to the ATCICA that a media request has been received. Any appropriate response to media requests will be developed and coordinated at the DA level. Each office should maintain the name and phone number of their current appropriate PAO and should ensure the local PAOs are also aware of this information.

"BIGOT" Cases and Close Hold Investigative Activity

2-65. In some instances, a case, due to its sensitivity or the sensitivity of the information involved, will require that it be handled on a strict need-to-know basis. These cases are often referred to as BIGOT cases because access to them is controlled by a BIGOT list. In this type of case, investigative actions are sometimes tasked directly to the field element by the ATCICA and all responses are returned directly to the ATCICA only. The ATCICA will notify the appropriate chain of command that a close-hold action has been initiated, identify the action element involved, and estimate the approximate degree of field element involvement. ATCICA will notify the chain of command upon completion of the close-hold action.

Handling Sensitive Compartmented Information Material in Investigations

2-66. All agents will keep their eyes open to the possible involvement of sensitive compartmented information (SCI) in their investigations.

2-67. Indicators that this might become an issue, include—

- Subject has a TS/SCI security clearance with SCI access.
- Subject is assigned to an intelligence unit or holds an intelligence MOS.
- Subject works in a sensitive compartmented information facility (SCIF).
- Reportable incidents that occur in SCIFs.
- The presence of unmarked information which deals with subject matter which has a high probability of being SCI (for example, SIGINT, HUMINT, cryptography).

2-68. Upon determining the involvement or potential involvement of SCI information in an investigation, the lead agent will coordinate with the local Special Security Office (SSO) for appropriate storage of the SCI information. The lead agent will wrap and seal the SCI material being stored in the SSO against access by personnel without the need to know.

2-69. Such protection will be afforded information until a final determination is made as to the classification of the information involved. If possible SCI material of investigative interest will be stored separately and in a security container accessible only by the CI special agents assigned to the case. A two-drawer safe, a drawer in a container where each drawer has a lock, or a "drop safe" are preferable.

2-70. The lead agent will notify the responsible ATCICA immediately upon determining the actual or potential involvement of SCI material in an investigation. All review and handling of SCI material involved in a CI investigation will be conducted in a SCIF. The Defense Courier Service and approved facsimiles (faxes) between SSOs are the only two authorized methods of transmittal of SCI material. The lead agent will contact the local SSO for assistance. The ATCICA will provide the lead agent with final disposition instructions for all SCI material obtained during a CI investigation. These instructions will include the procedures for addressing SCI material within a ROI.

Special Access Program

2-71. AR 380-381 governs the security of SAPs in the Army. A SAP is an approved security program imposing strict controls on individual access and dissemination of information. These controls are selectively applied to especially sensitive Army programs involving military research and development, activities, or operations. Agents will be familiar with the indicators of SAPs (for example, special handling instructions, special caveats, nicknames, and code words).

2-72. The ATCICA will be notified by the most expeditious means available regarding the involvement of SAP information in an investigation. AR 380-381 requires that the possible compromise of SAP information be reported within 24 hours to the Technology Management Office (TMO), HQDA. Whenever investigating agents encounter potential SAP material during the course of their duties, the material will be brought under immediate control, inventoried, and handled as evidence. Exposure to the material and knowledge of its involvement will be strictly limited.

SAP Read-On

2-73. The ATCICA and lead agent will identify the requirements for SAP read-on (additional agents, technicians, and desk officers) to conduct an investigation involving SAP material. Unless otherwise indicated, no SAP case will be run without read-on for key management and oversight personnel. This may include, but is not limited to, all CI special agents participating in or conducting investigative activities to support the investigation, command personnel as required and ATCICA or ACICA providing direction and oversight for that particular CI investigation. SAP read-on will be conducted with the appropriate SAP control officer.

Case Files

2-74. Two case files will be maintained on SAP investigations. One will be kept at the collateral level and the other will contain the SAP material. When an IMFR or other documents must contain SAP information, a dual reporting system will be followed. The investigating agent will submit two reports: one containing the SAP information and one containing collateral, sanitized information.

Reports of Investigations

2-75. On termination of the investigation, two ROIs will be prepared. One ROI will contain all case documentation, including the code word material. It will be retired through the TMO or the Special Records Information Activity (SRIA). The second ROI will contain only the sanitized material. This will be submitted through normal channels for retirement in the IRR. The collateral report will be a one-for-one match to the SAP report, unless a specific document cannot be included. In the latter case, a statement will be provided, generically describing the document and the information contained therein. The collateral version will make reference to the SAP version and provide a location, point of contact (POC), and telephone number for anyone required to view the complete record.

Security Procedures

2-76. SAP security procedures will be strictly adhered to in the conduct of a SAP investigation. Storage, handling, transmission and accountability of SAP information, physical security requirements, and other SAP security procedures will apply. Normal secure communication means is usually acceptable, as long as only cleared personnel are involved in the process (for example, a fax).

TERMINATION OR TRANSFER

2-77. **Terminated case files.** Upon receipt of a message from the ATCICA terminating investigative activity, the CI investigating element will take the following actions:

- If directed, an ROI will be completed and forwarded, along with all original signature investigative documentation and summary of information (SOI), to the responsible ATCICA.

- Ensure original signature investigative documentation includes the original CI incident reports, IMFRs, original exhibits, and originals of other documents predicating the investigation.
- Ensure supporting documentation is retained in the field dossier, including case logs, copies of the final correct CI incident report, ATCICA and ACICA message with operational interest determination, any tasking messages, copies of all IMFRs, documentation of any phone conversations between ATCICA and agent concerning the case, ACICA response memorandums, and copies of Summaries of Information.

2-78. **Open/Terminated (operational interest assumed).** Forward all original signature investigative reporting to the ATCICA. Retain supporting documentation for a minimum of one year from operational interest determination date. Due to OPSEC sensitivities, caution should be exercised in retaining theses file past the one-year mark. In no instance should follow-on coordination or support to the exploiting unit be filed with the original report.

2-79. **Open/Terminated (transferred).** Transferred CI cases occur when a CI investigation is initiated by one CI office (based upon ATCICA or ACICA approval) but a majority of the investigative activity will take place in another CI element's AO. In these instances, copies of the CI incident report (DA Form 2823 [Sworn Statement], and any ACICA correspondence transferring the case) will be maintained on file with the initiating CI element. All original documentation will be forwarded to the CI office designated as the lead investigating element by the ATCICA or ACICA. All transferred cases will be maintained on file until the case has been closed by the ATCICA or ACICA, the ATCICA or ACICA directs otherwise.

2-80. **Referred.** When information is determined to be under the purview of another agency, the information will be retained only long enough to refer the information to that agency. Forward all original signature investigative documents to the ATCICA upon transfer decision. No information concerning a U.S. person in referred cases will be retained in the local intelligence files. Referred cases containing no information on a U.S. person may be retained for as long as deemed necessary to support CI operations, subject to annual intelligence oversight inspections.

2-81. **Terminated (pending ROI).** Forward completed ROI (both hardcopy and softcopy) and all original signature documentation to ATCICA upon termination of investigative activity. Retain a complete copy of the ROI, all investigative reporting, and all supporting documents in the field dossier in suspense until notification of case closure (acceptance of ROI by IRR).

2-82. **Closed.** The lead element will maintain the complete field dossier until the date of destruction designated by ATCICA in the case closure message. Under no circumstances will the field element destroy a case file before this date without prior written approval of the ATCICA. The lead element will label the field case file with the following: "DO NOT DESTROY PRIOR TO _____." (Destruction date, normally one year from case closure for field dossiers, will be provided by ATCICA or ACICA in the case closure message.) The original field dossier may be retained past this date until no longer needed to support current operations not to exceed six years. Upon notification of a decision to prosecute or take adverse administrative action against the subject, place the field dossier back in suspense until action is resolved. Retention periods begin again upon notification completion of legal or administrative action.

2-83. **Case file destruction.** ARIMS allows longer periods of retention of field files and offers the agent wider latitude in what to keep. Files must be reviewed annually in accordance with AR 381-10. To ensure no important or original signature paperwork is destroyed, CI investigative elements will contact their ATCICA before destroying any investigative documents or material. The ATCICA will assist in determining if destruction is the appropriate action. Most problems with file destruction arise when CI investigating elements fail to forward original signature documents, copies of SOIs, or exhibits with IMFRs before case file destruction.

RECORDS CHECKS

2-84. The examination of files and records for pertinent information on the subjects of the investigation is the first action in most CI investigations. Records checks are conducted to identify indicators or anomalies

to substantiate or refute allegations or indications that a person or persons may be engaging in acts that constitute treason, spying, espionage, and/or subversion. Indicators and anomalies are based upon historical commonalities of persons involved in national security crimes, incidents of CI interest, or fit a profile of someone who may be cooperating with a FISS and ITO. Records checks should begin with local unit files and expand including a broad range of U.S. and HN law enforcement records that consist of civilian agencies that maintain records concerning the subject's personal background.

2-85. There are occasions when documented information or evidence is best obtained through other investigative means. Some recorded data could be wrong, out of date, or simply misinterpreted due to human error; however, the possibility of intentional deception or false information in both official and unofficial records must always be considered. Not all information contained in official government or civilian files should be considered absolutely true and should be corroborated via other records analysis and investigative activities.

2-86. If the record is to be used in a court or board proceeding, the manner in which it is collected, copied, extracted, or preserved will have a bearing on its use as evidence. Handling and storage for all information collected to support a CI investigation will adhere to the rules of evidence.

2-87. There is a risk factor with records checks. Exposure of the subject's name and the fact that he is under investigation may alert the subject. Due to the sensitivity of CI investigations, the subject's name may be submitted in a list of persons to mask the true focus of the records check and investigation. The investigating agent should examine all records requested and appear to review all records equally so the true target of the examination is not exposed to observant records custodians or other bystanders. CI special agents using this method during the course of approved investigative activities should exercise extreme caution to not use or retain any data on U.S. persons that would be in violation of AR 381-10, chapters 2 and 3.

GAINING ACCESS

2-88. A variety of procedural methods are available to the CI special agent to obtain access to and copies of records of investigative interest. The type of information being requested, the privacy rights afforded that type of information, and the nature of the agency holding it drive the decision on which method is appropriate. In general, government records are easier to get. Records of commercial companies are more difficult to obtain, often require formal written requests, and may require authorization by a high-level Army official, especially where specific privacy rights have been established in the law (for example, telecommunications and financial records). Checks can be either consensual or nonconsensual. Nonconsensual checks of records that have been afforded specific privacy rights under USC are the most difficult to obtain.

- **Informal request.** A verbal, or unofficial written request, by the CI special agent for access to records of interest. These requests are most often used for MACs and LACs where an existing liaison relationship exists and authority to access the records will not be questioned or can be established simply by the CI special agent's official status and authority with badge and credentials and regulatory reference.
- **Access with consent.** In cases where formal privacy rights have been afforded to a record, it can almost always be accessed with consent of the subject. Subjects may even be willing to give consent if they believe information in the record will refute, explain, or mitigate allegations against them. Usually this consent must be in writing and frequently, depending on the type of record, may require a specific form. This often occurs during the later stages of CI investigations, when the subject is already aware that he is under investigation.
- **Formal written requests.** Most national agency checks (NACs) and checks of commercial company records are requested formally in writing. Formal requests may take a number of forms. For example:
  - NACs are typically requested electronically or by memorandum, almost always through the ATCICA or ACICA.

  - Nonconsensual checks of commercial company records are requested by formal memorandum. These memorandums certify that the agency presenting them has the authority under a specific section of the USC to obtain the records and has met the legal thresholds required to exercise their authority. These memorandums are strictly formatted and often require specific approval authorities and signatures depending on the language in the supporting section of the USC Authorities differ depending on the type and subject matter of the record and the matters being investigated (for example, foreign CI versus terrorism).
  - Other formal written requests are simple requests for voluntary cooperation from commercial companies. These are used for travel related and general businesses. While the companies involved do not have to grant access, they are not prohibited by law from doing so.

- **Warrants, subpoenas, and court orders.** In some cases the only way to obtain access to a record is through a warrant or court order. This is the most formal method of obtaining access and is complex and time consuming. Warrants and court orders may be sought from military, federal, or the Foreign Intelligence Surveillance Court or a grand jury as appropriate. In joint investigations the Army will usually defer to the FBI to obtain a warrant or court order.
- **Access to records by MI investigators.** AR 381-20, paragraph 8-15a, provides regulatory authority for access to Army records. Upon presentation of badge and credentials, CI special agents will be permitted access to Army records under the provisions of AR 340-21, paragraph 3-1a, as required for the conduct of CI investigations or operations. Additionally, AR 210-10, paragraph 10-7, applies. They are also authorized to make extracts or transcripts of specific information obtained. Access to records of other Federal agencies is provided for in 5 USC 552a (b)(7).

2-89. Checks are generally categorized by whether they are conducted with a government agency or a commercial entity. Government checks are further divided into MACs or civilian government agencies. A distinction is also made between LACs and NACs. Checks of commercial companies which hold records of investigative interest are often described by topical category (for example, financial institutions, telecommunications providers, travel-related services). More importantly, however, is whether the USC has afforded specific privacy rights to that type of record and what exceptions have been allowed for CI and CT purposes under the law. For example, the disclosure of both financial and telecommunications records are generally prohibited with specific exceptions.

LOCAL AGENCY CHECK

2-90. A LAC is a records or files check of official or publicly available information retained by any local office or government agency within the AO of the field element conducting the check. These records may include holdings and databases maintained by local and state LEAs, local courts, and local offices of federal agencies. Some examples include files and databases maintained by—

- Local police departments.
- State police.
- Regional police and law enforcement networks.
- JTFs (for example, joint terrorism task forces [JTTFs]).
- State Department of Motor Vehicles.
- Tax assessment offices.
- Bureau of vital statistics (birth and death records).
- Voter registration records.
- Public utilities.

- Local courts.
- Local offices of the U.S. Postal Service.
- Local offices of federal agencies.
- Schools and universities.

MILITARY AGENCY CHECK

2-91. A MAC is a records or files check conducted at any military agency within the AO of the field element conducting the check. In accordance with AR 340-21, the DA Privacy Program allows disclosure of records to officers and employees of DOD who have a need for the record in the performance of their duties. This authority applies to records on Army installations. Military service records of current and past members of the armed services of most nations are detailed and usually accurate. MACs include, but are not limited, to the following:

- Personnel network.
- Joint Personnel Security Adjudication System.
- Unit and installation security manager.
- Unit S-1 and resource management officer.
- MP or PMO.
- Post Vehicle Registration Office.
- MP investigations.
- MP customs.
- Local and regional CID offices.
- Local offices of other military service law enforcement or intelligence offices.
- Military finance and personnel offices.
- Military medical facilities.
- Post Dishonored Check Office.
- Post education center.
- Civilian Personnel Office (employment and finance information).
- Post locator.
- Worldwide locator.
- Defense Eligibility Enrollment System.
- Defense Manpower Data Center.

MEDICAL RECORDS CHECKS

2-92. Medical record checks are considered a LAC or MAC depending on the status of the facility holding the record. For active duty military, the most readily available source for medical information is the servicing or local medical treatment facility. CI special agents should be aware that in-patient and psychological treatment records may be retained at the facility that provided treatment and may not always be fully reflected in outpatient records. For retired and separated Service members records may be located at the Army Personnel Center (ARPERCEN) records facility in St Louis, MO. Medical record checks should be done when one or more of the following exist:

- A suicide investigation. (This is rare and would usually be conducted as part of the USACIDC investigation.)
- Source states subject was directed for counseling for a problem which began to affect work habits.
- Information obtained during the course of the investigation indicates subject has been or is being treated for a medical condition or drug or alcohol problem to stop self-destructive behavior that was affecting work and life.
- Directed by ATCICA or ACICA.
- In a CSPE investigation for medical indication as to why the subject could not pass the polygraph examination (for example, effect of prescription medications).

2-93. CI special agents will **not** directly review medical records. The review will be done by the medical facility's reviewing medical officer. Information in psychiatric evaluation files generally will not be made available to special agents, but a medical authority will review and discuss the contents in general. It is suggested that Army Intelligence brief the medical officer before the review on what type of information Army intelligence needs out of the records. This is considered a record check even though the medical officer is doing the record review. The following information of the reviewing medical officer should be noted in introductory paragraph: Name, rank, position, medical facility name, and address.

2-94. If the subject is in possession of his medical record, discretely contact the commander of the medical facility and/or the subject's commander to have the medical records returned to the medical facility for review.

2-95. Should medical personnel refuse, attempt to determine if the file contains any type of information that would adversely affect the individual's suitability for access to classified information.

Note. In the above instance, the issue of suitability is related to the subject's possible inability to properly handle classified information or his willingness to compromise it.

CIVILIAN MEDICAL RECORDS

2-96. To conduct a check of civilian medical records, a warrant, subpoena, or written release from the subject is required. Civilian medical records are considered privileged information and will not be released to investigators except as indicated above.

2-97. Under no circumstances will previously executed personal records release forms (Defense Security Service [DSS] or OPM forms) from personnel security investigations be used in the conduct of CI investigations.

2-98. Any agent who determines that civilian medical, financial, or educational checks are required during the course of an investigation will submit an updated IP to ATCICA outlining the reason for the check.

2-99. If the records are deemed essential to the investigation, the ATCICA will assist in obtaining the required approvals or warrant.

NATIONAL AGENCY CHECKS

2-100. NACs are formal requests to federal agencies for searches of their records and supporting databases and files for information of investigative interest. NACs include DOD agencies as well as other federal agency holdings. NACs may be requested by the field element through the ATCICA. In accordance with local SOPs, the ATCICA will request NACs directly or through the ACICA and will submit and track all requests to other federal agencies at the headquarters level. Field elements will not attempt to initiate a NAC directly, with the exception of NCIC checks as outlined below. These types of requests add confusion to an already complicated process. Examples of national agencies that can be checked are listed below:

- DOD:
  - Defense Central Index of Investigations.
  - DOD IG.
  - Defense Manpower Data Center.
  - Defense Industrial Security Clearance Office.
  - Directorate for Industrial Security Clearance Review.
- FBI:
  - Criminal records.
  - Intelligence records.
  - FBI fingerprint checks (requires a fingerprint card).
- Bureau of Alcohol, Tobacco, Firearms, and Explosives.
- Federal Prison System.
- Federal Aviation Administration, DOT.
- Social Security Administration.
- CIA.
- DHS:
  - Immigration and Customs Enforcement.
  - Border and Transportation Security Agency.
  - U.S. Coast Guard.
- U.S. Treasury Department:
  - Internal Revenue Service.
  - U.S. Secret Service.
  - Financial Crimes Enforcement Center (FINCEN).
- State Department:
  - Security Division.
  - Passport Division.
  - Intelligence and Research Division.
- Military Departments:
  - Army.
  - Army Crime Records Depository (ACRD).
  - USAIRR.
  - National Guard Bureau.
  - Air Force.
  - Navy.
- OPM.

NATIONAL CRIME INFORMATION CENTER

2-101. While technically a NAC, in accordance with AR 381-20, all CI investigative elements will access and use NCIC terminals locally, wherever possible. On military installations NCIC access can usually be obtained at the local MP station, PMO, or installation security office. Access can also be arranged via liaison with local police departments, JTTFs, or other LEAs with NCIC access.

PROCEDURES

2-102. NACs are considered investigative actions and must be recorded by IMFR, regardless of the status of the investigation at the time the NAC results and/or investigative dossiers are received. Resulting IMFRs must be filed with the ROI. The IMFR for investigative dossiers will contain sufficient information in the introductory paragraph to identify the file for retrieval if necessary. The body of the report will contain sufficient detail to state the contents of the file, and not merely reflect that the file "contained no derogatory information," "no information pertinent to this investigation," or "no significant information." NACs are conducted and investigative dossiers are reviewed for information that will—

- Confirm or expand on information already known and/or reported.
- Determine known or suspected FISS and ITO affiliation.
- Attempt to identify someone.
- Obtain background or lead data.

COUNTERINTELLIGENCE INTERVIEWS

2-103. As part of their investigation, CI special agents conduct interviews. Each situation dictates the type of interview the CI special agent use when interviewing a subject:

- Noncustodial interview.
- Custodial interview.
- Walk-in interview.
- Source or witness interview.
- Subject interview.

NONCUSTODIAL INTERVIEW

2-104. Noncustodial interviews are conducted when subjects are interviewed without depriving them of their freedom in any significant manner (for example, arrest or detention). Subjects voluntarily consent to an interview and are advised that they may depart at any time. Exercise caution during these interviews so as not to impart suggestions of confinement or restraint, either through the type of room used (for example, bars on windows, locked doors), statements of the interviewing agent, or by the number of agents participating in the interview.

CUSTODIAL INTERVIEW

2-105. Custodial interviews are conducted when subjects are interviewed following a formal arrest or detention. Subjects are made fully aware of their deprivation of freedom or of their "in custody" status.

WALK-IN INTERVIEW

2-106. Interviewees are regarded as walk-in sources when they have knowledge of a national security crime or incident within the purview of Army CI, and they report their knowledge to the local Army CI office. The walk-in interview may provide information that results in a CI incident report.

SOURCE OR WITNESS INTERVIEW

2-107. Interviewees who may have knowledge of a national security crime or incident of CI interest are considered sources. Interviewees who may have actually witnessed a reported national security crime or incident of CI interest are considered witnesses. Persons providing access to records or any other type of documentation to support the investigation are also considered as sources. Depending on the attitude or association of the source or witness to the subjects, a source or witness can be cooperative, uncooperative, or even hostile.

SUBJECT INTERVIEW

2-108. The person who has committed or allegedly committed a national security crime or incident of CI interest is the subject. During CI investigations there can be one or multiple subjects. Due to the legal complexities involved in CI investigations and the potential for criminal proceedings, thorough preparation and consultation with the ATCICA, ACICA, and SJA should always be a priority to ensure all legal considerations and individual rights are observed and the prosecutorial integrity of the investigation is maintained.

INTERVIEW PREPARATION

2-109. Interviewing persons knowledgeable of, witnesses to, or involved in, alleged national security crimes or incidents within Army CI purview is the basis of all CI investigations. Interviews can successfully resolve suspected allegations when conducted meticulously and with all legal requirements or can jeopardize the ability to neutralize or exploit threats to national security. Thorough preparation for interviews is critical to establishing the CI special agent's authority and professional credibility to interviewees. While walk-in interviews cannot be planned, the CI special agent's knowledge of procedures, laws, policies, and investigative techniques will help during a walk-in interview.

SOURCE OR SUBJECT ASSESSMENT

2-110. After the initial walk-in, the investigating CI special agent will begin preparing for follow-on source and potential subject interviews. Agents must anticipate and mentally prepare for the interviews that may range from cooperative to hostile. Most walk-in interviews are cooperative since the interviewee is volunteering the information. However, source interviews may be cooperative or hostile depending on the attitude of the interviewee or relationship between the source and subject.

2-111. If interviewees are resentful of people in authoritative positions or have a close relationship with the subject, they may be uncooperative and hostile during the interview. The investigating CI special agent should be firm, but professional, and establish authority. Subjects in subject interviews are often uncooperative or hostile. People confronted with allegations of criminal activities are naturally defensive and confrontational. Senior-ranking subjects may be resentful of an interviewer or accuser whom they perceive is junior to them in age or rank. The investigating CI special agent should anticipate hostile reactions during subject interviews; however, these reactions should not impact professionalism or tactfulness during the interview. The CI special agent's professionalism, knowledge, and interpersonal skills are instrumental to manage the interview—induce interviewee cooperation and exploit interviewee's knowledge.

TELEPHONIC CONTACT WITH SOURCE OR SUBJECT

2-112. When making telephonic contact with a source or subject to arrange to coordinate an interview, the investigating agent has to balance security of the investigation while providing the minimum amount of information to induce cooperation. The CI special agent should conduct telephonic contacts as follows:

- **Identification.** Identify themselves and ask for the prospective source or subject's rank (if military) and name.

- **Source or subject identification.** Verify that they are talking to the prospective source or subject.
- **Reason for contact.** Explain they are investigating or conducting an inquiry into a security matter and that they would like to arrange to speak with the interviewee. Using verbiage like "matter of national security," CI special agent," or "CI investigation" may spook the prospective source or subject. The CI special agent will never provide details of a CI investigation over the phone.
- **Obtain agreement.** The prospective source or subject may believe he does not have any knowledge of an incident or security-related matter. The CI special agent needs to stress the importance of the interviewee's cooperation and that the prospective source or subject would be assisting the special agent in resolving a sensitive security matter.
- **Establish interview.** Establish the date, time, and location of the interview and ensure the prospective source or subject has directions to the interview. Ensure the prospective source or subject understands that the interview may last one to two hours. If the prospective source or subject is hesitant about being away from his place of employment for that long, offer other alternatives such as during lunch or before or after duty hours.
- **Provide security warning.** Advise the prospective source or subject of the official nature of the interview and that they are not to disclose their cooperation with anyone, including their supervisor. If they are adamant that their supervisor or chain of command should know, the special agent should obtain contact data for those persons and coordinate with the ATCICA for these contacts.
- **Provide re-contact information.** Provide official cellular or telephone numbers should the prospective source or subject need to contact the CI special agent before the interview.
- **Summarize.** Reiterate security warning, date, time, and location of the interview and thank the prospective interviewee for his time.

INVESTIGATIVE AIDS

2-113. CI investigative interviews are complex and time consuming. Regardless of the level of experience, investigating CI special agents should never go into an interview thinking they will be able to remember all the different protocols, legal warnings, and documentation required to complete an interview and still be able to effectively exploit all the information a source or subject may know.

2-114. Investigative aids assist in the exploitation of information. Investigative aids include Known and Unknown Person, Location, and Vehicle Identification sheets. CI special agents may also develop investigative aids for actions and objects (documents, electronic media) as these may likely be a part of a CI incident. Aids allow for full identification of persons involved in the incident that assist with future investigative activities, including records checks, and help in completing all documentation required during the investigation.

- Known person identification:
  - Name.
  - Rank and title.
  - Component.
  - Social security number.
  - Date and place of birth.
  - Duty position.
  - Duty location.

- Unit of assignment.
- Residence.
- Permanent change of station date.
- Temporary duty date.
- Expiration of term of service (ETS) date.
- Security clearance.
- Level of daily access to classified information.
- Special access—SCI only.

- Unknown person identification:
  - Sex—male, female.
  - Race—Caucasian, Black, Asian, Other.
  - Skin color—dark, tan, white.
  - Skin complexion—smooth, pock-marked.
  - Age—within a 5-year range.
  - Height—within a 2-inch range.
  - Weight—within a 10-pound range.
  - Build and posture—small, medium, and stooped.
  - Hair—black, brown, grey, blond, red, bald.
  - Eyes—brown, black, blue, grey, green.
  - Dress—headwear, upper- to lower-body wear, foot wear, jewelry (top to bottom).
  - Distinguishing characteristics—physical handicap, tattoos, body piercing, scars, birthmarks, moles.
- Location identification:
  - Room number and name.
  - Floor number.
  - Building number and name.
  - Street address (intersection).
  - Nearby landmarks.
  - Surrounding area description.
  - Installation.
  - City.
  - State.
  - Country.
  - ZIP code.

- Vehicle identification:
  - Make.
  - Model.
  - Year—can use time span.
  - Color.
  - License plate number.
  - License plate state.
  - Distinguishing characteristics—stickers, damage, other.
  - U.S. military installation decals—include associated color labels denoting, civilian, enlisted, officer.

INTERVIEW AGENDA

2-115. An interview agenda is another type of investigative aid that allows investigating CI special agents to decide how they want the flow of the interview to go. Interview agendas allow investigating CI special agents to manage the interview and serve as a road map to key them on the completion of mandatory documentation and security warnings required during the interview process.

2-116. Interviews are conducted based upon the experience level of the investigating CI special agent and how he likes to transition between different topical areas. For example, some investigating CI special agents like to complete all administrative documentation (for example, Privacy Act of 1974, Secrecy Affirmation) at the beginning of the interview, complete information exploitation, and follow up with executing the Sworn Statement and final security warning. Other investigating CI special agents may prefer to conduct all the information exploitation, get source data, cover all administrative documentation, and then execute the Sworn Statement and issue the security warning.

2-117. When using interview agendas, the investigating agent should always keep it concealed or out of sight. If a source recognizes the agent is relying on this document to complete the interview, it may undermine the credibility and professionalism of the investigating agent, and may result in the source being more cautious, confrontational or uncooperative. The amount of detail the agenda contains is left to the discretion and amount of experience of the investigating CI special agent. The following is an example of an interview agenda:

- ID source.
- Present badge and credentials.
- Synopsis of the information.
- Detailed account of the incident by the source.
- Use of Interrogatives.
- Privacy Act of 1974.
- Secrecy Affirmation.
- Sworn Statement.
- Security Warning.

INTERVIEW ROOM SETUP

2-118. It is important to determine what physical setting or environment will be most conducive to gaining the trust and confidence of the source and will produce the most truthful and meaningful information. Interviews can be and frequently are conducted in a myriad of settings, locations, and environments. It is completely acceptable to conduct an interview at a source's place of work, home, or other location where he may feel more comfortable. Comfort sometimes allows a subject to talk more openly and freely, which can greatly benefit the investigative process.

2-119. A subject interview needs to be strictly planned and controlled. A subject interview should rarely, if ever, be conducted in an area where the subject works, socializes, or feels secure. The location selected for a subject interview should provide complete privacy (free from distraction or disruption). Interview rooms should not be equipped with phones, outside windows, wall ornamentation, and so forth. In addition to these requirements, the room should be strategically arranged to ensure the most practical and conducive environment. If the room is equipped with a two-way mirror, the subject should not face directly toward it. This serves as a constant reminder that someone may be monitoring the interview.

2-120. Interview rooms should be equipped with a desk and at least three chairs if using an assisting agent or four chairs if an interpreter is used. The interviewing CI special agent should be located directly across from the interviewee. If an assisting agent is used for note taking or witnessing, they should be located to the side of the interviewing CI special agent, far enough away so they are not in direct line of sight of the interview.

2-121. When possible, the interview chair should be a four-legged chair with no arm rests. This removes any potential psychological barriers or defense mechanisms and allows for easier recognition of body posture and physiological indicators of deception during the interview. Additionally, investigating CI special agents should use a hydraulic-type chair to manipulate their level above the interviewee to establish a psychological dominance and position of authority. If using an interpreter, they should be placed to the side and slightly behind the interviewee to ensure that their focus is directed towards the investigating CI special agent. If the room is equipped with video recording equipment, it should be mounted in a corner with visibility on the interviewee's face, yet still out of direct eyesight so that it is not a distracter. Figure 2-3 shows an example of a room setup.

RECORDING INTERVIEWS

2-122. As a general rule, Army CI does not record interviews. Taping interviews requires prior written approval of the responsible ATCICA. The ATCICA will coordinate this action with the unit intelligence oversight officer and SJA. A careful risk or gain assessment must be done to ensure the benefits expected by taping the interview outweigh potential risks to the investigation. There is a significant logistical and administrative burden involved with such activities.

2-123. Additionally, when the intent of an investigation is to prove a criminal act, a written report accompanied by an incriminating signed sworn statement is sufficient. No value is added by including a recorded confession. More often than not, the recording becomes a target for the defense to accuse wrongdoing on behalf of the investigating agency or prosecution. Interviews and debriefings of subject as part of a plea bargain or after the trial is complete for the purpose of conducting damage assessment are common. Taping interviews should be considered when—

- Interviews are conducted in foreign languages.
- An interpreter is used.
- Interviews are lengthy.
- Interview topics are technical or extremely complicated in nature.

Information Exploitation

2-124. At the beginning of an interview, the investigating agent will have the interviewee provide a detailed explanation of the incident starting with the earliest relevant date and time concerning the incident. The investigating CI special agent will not interrupt and will take very few notes. This helps the interviewee refresh his memories and mentally recount the incident. After this initial dialogue, the investigating agent will have the interviewee go back to the beginning of the incident and slowly have him or her recount the details while the investigating agent takes detailed notes.

2-125. The interview should flow sequentially to develop a logical time line of what happened. As the interviewee provides details concerning the incident and reveals other information, the special agent should make a note and follow-up with a separate line of questioning of that lead or string after the current topic has been fully exploited.

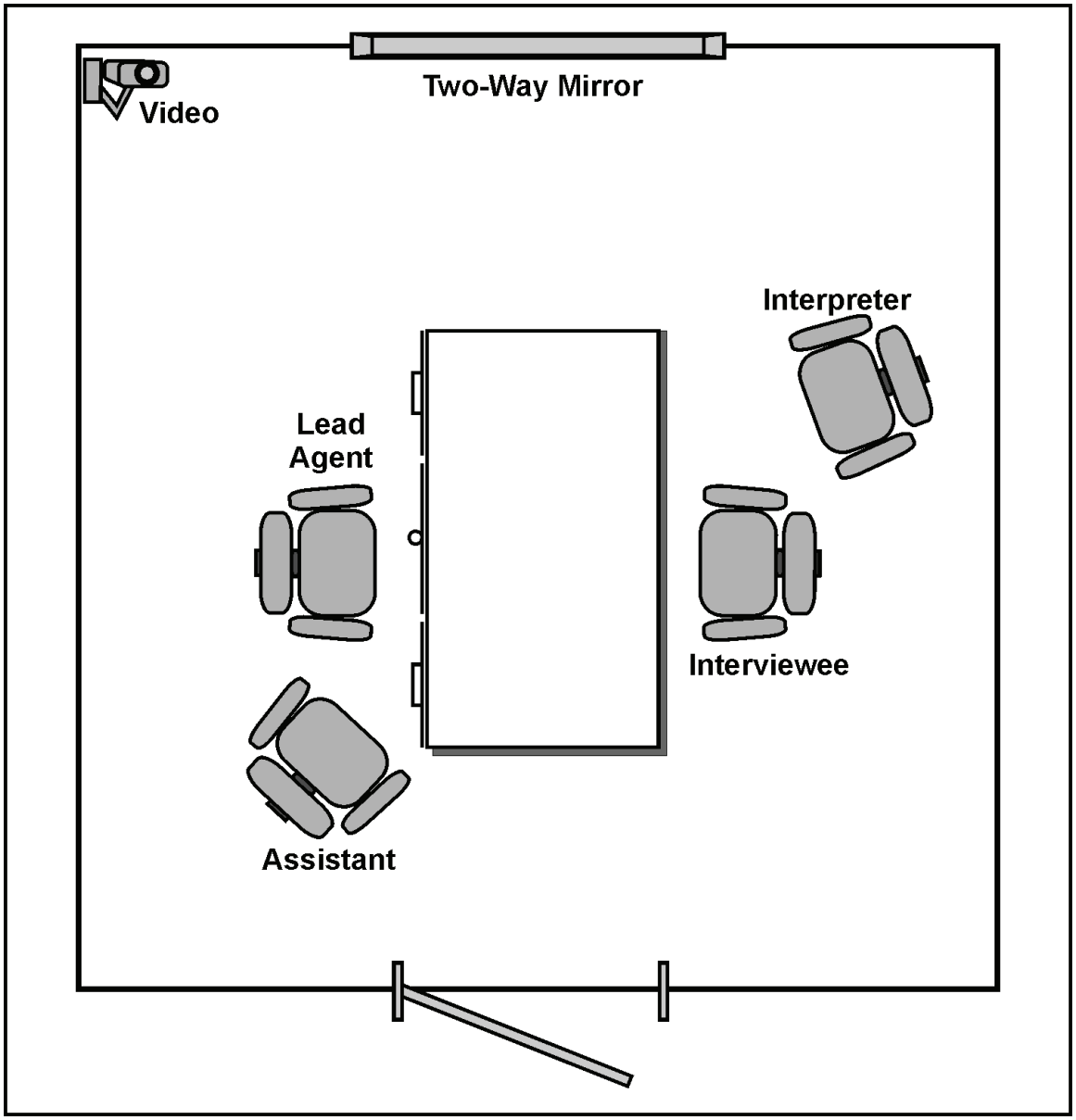

Figure 2-3. Example of an interview room setup

2-126. When asked for specific dates, times, and locations, the interviewee may not be able to provide exact information. In this case the investigating CI special agent needs to identify the details as precisely as possible. If the interviewee cannot remember a specific date, the agent needs to gradually broaden time spans to a day of the week, week, month, or time of year, or even season, to get the most precise information available.

Note Taking

2-127. Accurate, detailed, legible, and properly sequenced notes are critical in articulating the information obtained during all interviews. During the interview, as information is developed, if the interviewee provides another lead or string that requires exploitation, make a note in the margin, fully develop the current topic, and go back and exploit the lead or string provided earlier. This helps maintain the tempo of the interview, limits interviewee confusion by disrupting a sequence of events, and makes it easier to transcribe the notes into a report or sworn statement. If the interviewee is providing details about a specific event and mentions a name, for example, "John", do not interrupt to request John's personal identifying information. Make a note. After exhausting the current topic, go back and follow-up with questions concerning John.

Backup Information

2-128. Part of the interview preparation is to have prepared copies of all administrative and legal documentation that may be required in a particular interview. These include copies of the Privacy Act of 1974, DA Form 2823 (Sworn Statement), DA Form 3881 (Rights Warning Procedure/Waiver Certificate), and Consent to Release Forms and Secrecy Affirmations. The investigating agent should have blank copies of all these documents available as well as ones that have all areas that require signatures and/or initials highlighted to ensure they are properly documented during the interview. Copies of the DA 3881 should also be available during walk-in and source or witness interviews since there may be times when these interviewees, although cooperative, may implicate themselves in a criminal offense. During subject interviews, investigating CI special agents should also have a copy of all charges (Title 18, USC, and UCMJ) available to explain why their suspected actions are viewed as criminal offenses.

Questioning Techniques

2-129. How an investigating CI special agent asks questions in an interview is also important. Good questioning techniques limit confusion of the interviewee; maintain the tempo and control of the interview; and save time by limiting repetitive clarifying questions.

2-130. Direct questioning using the basic interrogatives *who*, *what*, *when*, *where*, *why*, and *how*" is the most efficient way to exploit information in most interviews. Investigating CI special agents will never use compound or leading questions. The investigating agent should avoid asking questions like these:

- **WRONG.** Can you spell John's name? This creates two questions and two answers. The initial question and the answer, which will usually be *Yes* or *No*, and the follow-up question, spell John's name.
- **RIGHT.** Spell John's name.
- **WRONG.** You saw John take the classified document home, right?
- **RIGHT.** Who took the classified document home; or did you see John take the classified document home?
- **WRONG.** Was John in the office and who was with him?
- **RIGHT.** Was John in the office? (After the answer, ask the follow-up: Who was with him?)

2-131. Elicitation is the use of generalized questions to ascertain someone's knowledge on a particular topic. In some cases of source or witness interviews where it is unknown whether the interviewee has knowledge concerning the incident, it may be necessary to begin elicitation to ascertain his knowledge of

the incident. If the interviewee has no information concerning an incident under investigation, then the investigating CI special agent will not have given away any circumstances surrounding the incident that could be compromised later on.

2-132. To elicit an interviewee's knowledge, the interviewing agent may simply ask, "do you know of any security incident that may have happened in a specific timeframe?" or "where were you on this date and did you notice anything suspicious?" Once the interviewee has acknowledged knowing about the incident in question, the investigating agent may then begin asking direct questions.

INDICATORS OF DECEPTION

2-133. Detection of deception is not a simple process, and it normally takes years of experience before a CI special agent can readily identify deliberate deceit. Inconsistencies in the source's actions or words do not necessarily indicate a lie, just as consistency is not necessarily a guarantee of the truth. However, a pattern of inconsistencies or unexplainable inconsistencies normally indicate deceit.

Internal Inconsistencies

2-134. Frequently when an interviewee is lying, the investigating CI special agent will be able to identify inconsistencies in the time line, the circumstances surrounding key events, or other areas within the questioning. For example, the interviewee may spend a long time explaining something that took a short time to happen, or a short time telling of an event that took a relatively long time to happen. These internal inconsistencies often indicate deception.

2-135. Body language does not match verbal message. An extreme example of this would be the interviewee relating a harrowing experience while sitting back in a relaxed position. The investigating CI special agent must be careful in using this clue since body language is culturally dependent. Failing to make eye contact in the United States is considered a sign of deceit while in some Asian countries it is considered polite.

Lack of Extraneous Detail

2-136. Often false information will lack the detail of truthful information, especially when the lie is spontaneous. The investigating agent needs to ask follow-up questions to obtain the detail. When the interviewee is unable to provide the details that he knows, it is an indicator of deceit. If the interviewee does provide this additional information, it needs to be checked for internal inconsistencies and verified by repeat questions.

Repeated Answers with Exact Wording and Details

2-137. Often in the case of subjects, if he plans to lie about a topic, the subject will memorize answers or details. If the interviewee always relates an incident using exactly the same wording or answers repeat questions identically (word for word) to the original question, it may be an indicator of deceit. In an extreme case, if the interviewee is interrupted in the middle of a statement on a given topic, he will have to start at the beginning to "get his story straight."

Physical Cues

2-138. The interviewee may display physical signs of nervousness such as sweating or nervous movement. These signs may be indicators of deceit. The fact that an individual is being questioned may in itself be cause for some individuals to display nervousness. The investigating agent must be able to distinguish between this type of activity and nervous activity related to a particular topic. Physical reaction to a particular topic may simply indicate a strong emotional response rather than lying, but it should key the agent to look for other indicators of deceit.

2-139. Failure to answer the question asked. When an interviewee wishes to evade a topic, he will often provide an answer that is evasive and not in response to the question asked. For example, if the interviewee

is asked, "Were you in the office when the document was taken?" and he replies, "I was in the office that day," he has truthfully answered a question, but has avoided being put into a position that may implicate him in the incident. Or when a person repeats a question, it may be a stall tactic while trying to think of a plausible answer to the question.

Source Confidentiality

2-140. Sources may be reluctant to talk to CI special agents based on a fear of becoming involved in a legal proceeding, having to face cross-examination, or reprisal by the subject. Rapport building, reassurance, appeals to duty and encouragement to do the right thing are the preferred method for obtaining cooperation.

2-141. However, if a source is still apprehensive about cooperating, investigating CI special agents can, under the provisions of the Privacy Act of 1974 protect source's identity and grant confidentiality to ensure the source's identity is not revealed outside official or law enforcement channels. This protection would include any documentation petitioned from external agencies outside law enforcement and military channels under the FOIA. The Privacy Act of 1974 caveat and requests for confidentiality will be annotated within investigative reports. Confidentiality should be offered as a last resort, and not until it is apparent to the investigating CI special agent that rapport building, reassurance, appeals to duty, and encouragement to do the right thing do not dissuade the source's reluctance to provide answers to the investigating CI special agent's questions.

REQUIRED VERBAL WARNINGS DURING INTERVIEWS

2-142. The following verbal warnings are required during interviews:

- **Security Warning (to be administered to all interviewees after each interview session).** "Sir/ma'am, the matter that we have discussed today is regarded by the Department of the Army as extremely sensitive in nature. In order to protect the integrity of this investigation, we request that you not discuss this matter with anyone outside the official investigative channels of this office. Thank you for your cooperation."
- **Follow-Up Security Warning (given at the end of follow-up interviews with the same person).** "I want to thank you again for not discussing this official and very sensitive matter with anyone outside the official investigative channels of this office."
- **Telephonic Security Warning.** "Despite the fact that I have provided you with limited information concerning this matter, I ask you not to discuss this matter outside the official investigative channels of this office. Thank you for your cooperation."
- **Consent to Release Under the FOIA.** "I need to inform you that the information we have discussed today will be made into an official report and that report will become part of official U.S. Government files. Under the provisions of the Freedom of Information Act, any U.S. person mentioned in this report may request a copy of those files once the case is closed, adjudicated, and made a part of official U.S. Government records. Do you have any objections to having your name released as the provider of this information?" (Use this warning for walk-in and source only.)
- **Oath of Truthfulness for Subject Interviews.** "The Department of the Army desires that this interview be conducted under oath. Are you willing to be interviewed under oath? Do you swear or affirm that the information you are about to provide in this interview is the truth, the whole truth, and nothing but the truth?"
- **Title 18, USC for Perjury Warning for Subject Interviews.** "I must inform you that under the provisions of Title 18, USC, or Uniform Code of Military Justice (depending upon the status of the interviewee), if you willingly and knowingly provide false or misleading information, you could be subjected to additional criminal charges and penalties punishable by 5 years of imprisonment or fined or both. Do you understand this?" (Request signature.)

CONDUCTING THE WALK-IN INTERVIEW

2-143. Walk-in interviews are conducted when a person voluntarily approaches a CI special agent to report an incident of CI interest or national security crime within the CI investigative authority and jurisdiction. During the walk-in interview, the CI special agent thoroughly develops the information provided by the volunteer to identify specifics of the incident (dates, times, locations), description or identity of a witness or person with knowledge of the incident, and the description or identity of the persons involved in the incident. There are four phases of the walk-in interview:

- Approach.
- Information development.
- Sworn statement.
- Termination.

Approach Phase

2-144. The approach phase of the interview allows the CI special agent to confirm the source's identity, to introduce himself to the source, and to assure the source that he is in fact talking to a representative of the appropriate agency. Specifically—

- Receive the source into the office and tell them who you are. It is not necessary to present yourself as a special agent, or even your military affiliation, at this time. For example, "Hi. My name is.... What can I do for you?"
- Allow the source to provide a brief summary of the incident he wishes to report. Do not take copious notes at this time because the information may not be in CI jurisdiction.

2-145. Any source (walk-in, telephone caller, or written message) who volunteers information, the collection of which is unauthorized by AR 381-10, will be referred to the proper authorities. These sources and the information they provided are referred to as unsolicited sources and unsolicited information. If possible, all unsolicited sources will be fully identified and, if the information volunteered is of no interest to Army intelligence but may be of interest to another agency, the source will be referred to the appropriate agency.

2-146. Once you have determined that the source has a genuine need to talk to a CI special agent, identify yourself as such and show him or her your credentials. In return, request the source's military ID Card, or picture ID, to ensure his identity. Ensure the source matches the description and photograph on the ID card.

2-147. If the individual provides information that reveals a potential threat to a high-level Government official, the information must be reported through command channels.

Information Development Phase

2-148. This phase allows the special agent to clarify information, identify and exploit information of CI interest, pursue leads, develop any espionage indicators, and obtain sketches if necessary.

Clarify All Information

2-149. An example of clarifying all information would be if the source informs you of a vehicle that was identified during the incident. Attempt to obtain all descriptive data on the vehicle. Persons not known by name to the source must be identified by description (sex, height, weight, manner of dress, hair color, eye color, and any distinguishing marks).

Pursue Leads

2-150. Ascertain who else was in the area at the time of the incident or who else has knowledge of the incident. Attempt to identify these individuals and where they work. By talking to several people that were in the area at the time of the incident, accurate facts can be obtained and a logical conclusion can be made.

Develop Espionage Indicators

2-151. Fully develop any espionage indicators. Espionage indicators provide a general idea as to the type of individual that may be investigated. The source may not have personal knowledge of the subject; however, ask the source if he has any knowledge about the subject concerning the following:

- **Finances.** Have they received any letters of indebtedness or unpaid bills? Do they have any financial problems? Do they have a problem paying bills? Do they appear to be spending more money than they make?
- **Life-styles.** Do they live life "in the fast lane"? Are they quiet individuals who keep to themselves? What interests do they have?
- **Hobbies.** Have they ever talked about their likes or dislikes outside the workplace? Do they collect any objects? Do they belong to any organizations outside the military?
- **Associates.** With whom do they associate during the duty day? With whom do they associate after duty hours? With whom do they work? Who can provide more information concerning subjects?
- **Foreign connections.** Do they have any U.S. relatives living abroad? Do they have any foreign contacts, business connections, own any foreign property?
- **Foreign travel (other than official military travel).** What foreign travel have they taken? Where do they go? How often to they travel? What are there reasons for traveling abroad?
- **Loyalty and allegiance.** Do their personal beliefs, statements, actions, or associations indicate they may not be loyal to the U.S. military or Government?
- **Work habits.** Do they have the combinations to the security containers in the office? Have they ever had any security violations? Do they volunteer for extra work? Do they volunteer for sensitive assignments? Do they excessively use the copier? Have they ever been cited for a security violation? Do they often work late or come in to work early? Are they signed for a set of keys to the building or office?
- **Emotional, mental, and personality disorders.** Do they have any known or suspected emotional, mental, or personality disorders that may affect their behavior or actions or cause them to be susceptible to influence or coercion?

2-152. A sketch of the incident area generally assists in understanding the incident, as well as allows time to formulate additional questions. Ask the source to provide a sketch of the area; ensure that all markings on the sketch are those of the source. The following are some basic guidelines for sketches. Have the source—

- Title the sketch and annotate the date and time of the location of the incident.
- Indicate the compass direction North if the sketch is of an outside location. If the direction is not known, use cross-street information.
- Indicate where all persons involved were located.
- Indicate any obstacles that would have deterred their line-of-sight to the incident.
- Print their full name, sign, and annotate the date the sketch was drawn.

2-153. After all the information has been fully developed, review your notes with the source to ensure you have accurately annotated all information. Remember to ask the source if he has any further information to add.

Sworn Statement

2-154. Request a DA Form 2823. The best policy is for the investigating CI special agent to type the sworn statement from the notes of the interview. Have the source check for accuracy, correct any mistakes, and have the source sign the DA Form 2823. It is allowable to have sources hand write their own sworn statement. Make arrangements for the source to return and sign the sworn statement after it is prepared by the CI special agent. Upon final execution of the sworn statement, reiterate the official and sensitive nature of the investigation.

Termination Phase

2-155. During this phase, the special agent will finalize all the administrative procedures and ensure he has all the necessary information to complete the reports. In particular—

- Have the source read the provisions of the Privacy Act of 1974 and answer any questions he may have about it.
- Obtain a full identification of the source. Basic identification includes full name, SSN, military rank or civilian pay grade, date and place of birth, duty position, unit of assignment, place of residence, ETS, date of last CI awareness briefing, and security clearance.
- Ask the source why he reported the incident. Sometimes, the source's motivation may provide more insight as to the validity of the information. Some of the basic motives why individuals report possible CI incidents to CI include ideology, compromise (fear or protection), and ego (revenge or elitism).
- Ask the source if he has any objection to your contacting him for further information. If the source has no objection, ask if he prefers to be contacted at work or at home. If the source does have objections, try to inform the source that the information discussed should be considered as a part of an official CI investigation, and the details of the interview or the information concerning the incident are not to be discussed with anyone else.
- Inform the source that the information can be obtained through the FOIA and explain the consent to release process. If the source has already talked to several individuals, get identifying information on them to list in the report. Normally, it is not desirable to have numerous individuals know about an incident or pending or ongoing investigation. The fewer people who have knowledge of the incident (outside official channels), the less chance there is of a compromise.
- Give the source a Security Warning and have him sign a Secrecy Affirmation Statement (or Non-Disclosure Agreement).
- Thank the source for the information provided.

CONDUCTING A SOURCE OR WITNESS INTERVIEW

2-156. Sources or witnesses are those persons who may have observed, heard, or have knowledge of a CI incident or national security crime within CI investigative authority and jurisdiction. Sources and witnesses are normally identified during the conduct of a walk-in interview. Source or witness interviews are conducted using the same basic principles used in the conduct of a walk-in interview.

Approach Phase

2-157. During the approach phase, the CI special agent confirms the source's identity. After introductions, the CI special agent determines whether the source has knowledge or information regarding the CI

investigation. Conducting a source interview is similar to conducting a walk-in interview. CI special agents—

- Identify themselves, first, by using their special agent credentials—name and organization—and then by showing their credentials to the source.
- Identify the source or witness by verbally verifying the source or witness's name and rank and requesting picture identification, such as a military ID card. Identity verification is at the CI special agent's discretion.
- Explain the purpose and official nature of the interview and ensure explicit investigation details are not revealed.

2-158. Determine if the source was at the location of the incident during the reported timeframe or if he has any knowledge concerning a security incident at a particular location during a specific timeframe. If he was or does not have any information, ascertain if he knows of anyone who was there. Ask why someone would believe that he was there.

2-159. If the source states that he was at the scene, proceed with the interview. Ensure that the source understands that the U.S. Government considers his presence and all matters discussed during the interview to be official in nature and they are not to be discussed with anyone outside official channels. Determine if the source has discussed the incident with anyone and tell the source that he is not to discuss the matter further.

2-160. Provide the source with the appropriate Privacy Act Advisement.

Information Development Phase

2-161. This phase allows you to clarify information, identify and exploit information of CI interest, pursue leads, develop any espionage indicators, and obtain sketches if necessary. Ask direct questions that elicit narrative responses.

2-162. If the case is such that the number of those knowledgeable of the issue is very limited, or, if the lead sheet specifies the conduct of a discreet investigation, the source interview may require some changes in conduct including the following:

- Ask indirect questions that will elicit the appropriate responses.
- Use methods to conceal the identities of other sources to prevent the source from finding out the issue at hand. **Never lie to the source.**
- Allow the source to tell his story in narrative format all the way through. Note taking should be kept to a minimum. Focus your attention on the source and listen to his story.
- Do **not** make any promises other than a promise of confidentiality.
- Ask clarifying questions. Review the story with the source to ensure that you have the complete story. Do not assume that you know what this source means or knows, based on previous information or interviews.
- Cover all information. All information or incidents previously brought to your attention should be fully covered to ensure that you have this source's observations. Any new information the source identities should be fully developed. Basic questioning techniques come in to play. The six basic interrogatives form the basis for you questions.
- Fully develop espionage indicators of finances, lifestyle, hobbies, associates, foreign relatives, foreign travel, and work habits (see figure 2-2 [page 2-13]).
- During the interview, determine if there are any new leads and fully identify leads mentioned by the source.

- Obtain full identification of the source. Basic identification includes full name, SSN, date and place of birth, duty position, unit of assignment, place of residence, home and work telephone numbers, ETS, and security clearance. Before obtaining the SSN, ensure you have provided a Privacy Act of 1974 statement covering the four main points.
- Review your notes before asking for a sworn statement.

Sworn Statement

2-163. Request a DA Form 2823. The best policy is for the investigating CI special agent to type the sworn statement from the notes of the interview. Have the source check for accuracy, correct any mistakes and have the source sign the sworn statement. It is allowable to have the source hand write his own sworn statement. Make arrangements for the source to return and sign the sworn statement at a later date and time if required. Upon final execution of the sworn statement, reiterate the official and sensitive nature of the investigation.

Termination Phase

2-164. During this phase, the special agent will finalize all the administrative procedures and ensure he has all the necessary information to complete the reports. In particular—

- Determine if the source has any objections to being re-contacted. Verify his resident address and home and work telephone number for re-contact if not obtained while developing all of their personal information.
- Reiterate security by reminding the source of the official nature of the interview and the matter discussed.
- Issue the Consent to Release.
- Issue the Secrecy Affirmation.
- Thank the source for his time and cooperation.

CONDUCTING THE SUBJECT INTERVIEW

2-165. Subjects are those persons suspected to be involved in a CI incident or national security crime within CI investigative authority and jurisdiction. Subjects are normally identified during the walk-in or source or witness interviews. Although the subject interview is conducted using the same basic principles as the walk-in and source or witness interviews, there is more legal coordination conducted before the interview. The subjects are advised of their rights before questioning them regarding the incident or crime.

Approach Phase

2-166. The approach phase allows you to confirm the subject's identity through verification of a form of identification. Introduce yourself as a CI special agent and present your badge and credentials and explain the circumstances of the interview. The approach phase for the subject interview differs from the walk-in and source or witness interviews in that you need to advise the person of their rights due to the allegations involved. The subject interview is predicated on exhaustion of all other interviews and investigative activities (unless otherwise directed by the ATCICA), approval of a SIP by the ATCICA, and prior coordination with the SJA and appropriate authorities if detention is anticipated.

Note. Go over hypothetical situations. subject may state he did not do it, or refuse to talk, or admit he is guilty, become hostile or confrontational, or confess to a crime you knew nothing about. Be prepared to handle any of the situations that may arise. Know what your authority is and be prepared to exercise that authority.

2-167. Explain to the subject the general purpose of the interview and reiterate the confidential nature of the interview. Inform the subject you have received information indicating him as a subject in a CI investigation. The interview allows him the opportunity to explain, refute, or mitigate questionable or misleading information received during the conduct of the investigation.

2-168. Administer DA Form 3881. Do not question the subject until proper advisement of legal rights and voluntary waiver of those rights has been accomplished. Request subject read and sign a DA Form 3881 to acknowledge receipt of the explanation of rights and record the individual's decision to exercise or waive the right to remain silent and to consult counsel. It is suggested to administer the rights advisement early in the interview because of the details of the suspected or accused charges involved, and this is usually the peak of anxiety for the subject.

2-169. Once the subject agrees to talk with you, the tension in the interview will generally, not always, subside. If the subject invokes his rights upfront, your time will not have been wasted in delaying the circumstances of the interview while having him fill out all the other documentation. Even if the subject waives his right to counsel initially, he can invoke his rights later in the interview. When this occurs, you **must stop** questioning the subject and consult with SJA on disposition.

- **Perjury Warning Provisions of Title 18, USC** Before questioning the subject concerning the allegations, inform the subject of Title 18, USC "I need to inform you of Title 18, United States Code. Should you willfully provide false information, you could be subject to a $5,000 fine, up to 10 years in prison, or both."
- **Privacy Act Advisement.** Have the subject read the Privacy Act Advisement. Verbally inform subject that the Privacy Act of 1974 requires that each individual who is asked to provide personal information be advised of the following four salient points:
  - Authority by which the information is being collected.
  - Principal purpose for which the information will be used.
  - Routine uses for the information.
  - Voluntary nature of disclosing information and the possible repercussions of failure to do so.

Note. Have the subject sign a copy of the Privacy Act Advisement to retain for your records. If subject wants a copy, provide it.

Information Development Phase

2-170. When conducting subject interviews, consider the following:

- Do not make off-the-record or unofficial remarks in the interview or any promises or commitments to subject that are beyond your legal authority.
- Avoid statements or representations which may be construed as opinion or advice to the subject about past, present, or future actions. Do not argue with the subject or express personal viewpoints on any matter.
- Interview and question the subject concerning the matter under investigation. Use your interview plan and the questions you developed during your planning and preparation process to fully explore and develop the area of interest to establish the facts surrounding the allegations.
- Use basic interview techniques. When questioning the subject, it is imperative you obtain direct responses to ALL allegations. Verify and complete previously developed information; after which, fully develop any other and all information.

- Review your notes. When you are confident all investigative requirements are satisfied and all the information has been fully exploited, inform the subject that you are going to review your notes together to ensure accuracy. If there is anything you forgot or have incorrectly recorded it, give the subject the opportunity to clarify or provide additional information. Review your notes whenever you feel it is necessary to clarify information provided.

Sworn Statement

2-171. Request a DA Form 2823 from the subject. The best policy is for the investigating agent to type the sworn statement from the notes of the interview. Have the subject check for accuracy, correct any mistakes, and have the subject sign the DA Form 2823. If the subject refuses to sign the sworn statement, annotate that on the form, sign it, and retain it in the dossier. It is allowable to have the subject hand write their own sworn statement. The subject's sworn statement will be prepared before rendering any decision on the disposition (release or detention) of the subject.

Terminate the Interview

2-172. When terminating the interview, address the following:

- **Ask the "catch-all" question.** When you are confident all investigative requirements are satisfied and all relevant and/or derogatory information has been fully exploited, ask the subject if there is anything he would like to add to the interview. If the subject adds something, record the information and continue to ask the question "Is there anything else you wish to add?" Repeat this line of questioning until a negative response is obtained.
- **Polygraph.** Ask the subject if he is willing to submit to a polygraph examination.
- **Security warning.** Provide the subject with a security warning (Non-Disclosure Statement). State "I need to remind you that the information we have discussed during the interview is to be considered confidential and official in nature and should not be discussed with anyone outside the investigative channels of this office."
- **Thank the subject.** To maintain the established rapport, thank the subject and terminate the interview.
- **Determine proper disposition of subject (release or detain).** If the anticipated direction of the interview has changed, consult with SJA before making a final decision on the disposition.

COUNTERINTELLIGENCE INVESTIGATIVE REPORTS AND FILES

2-173. Personnel involved in CI operations and CI or CE investigative activity will maintain complete and accurate records. Records will be maintained in accordance with the ARIMS contained in AR 25-400-2.

LOCAL INVESTIGATIVE CASE CONTROL LOGS

2-174. To facilitate tracking, storage, retrieval, and suspense of records pertinent to CI investigative activities in their AOR, all investigative elements should maintain case control logs reflecting all investigations of all types and scope including RFAs. Case logs may contain as many fields as necessary for local needs. Common fields include cross-references to FBI and other agency control numbers, nicknames when assigned, and nicknames for supporting source operations or special collection techniques when assigned. At a minimum these logs will contain the following items of information:

- Local case control numbers (LCCNs).
- ACICA control numbers (ASCCNs).
- Incident or personal subject block.
- Case opening date.

- Current case status (including date for OPEN or SUSPENDED, OPEN or TERMINATED, REFERRED and CLOSED investigations).

FIELD DOSSIER

2-175. The most important investigative file is the field dossier, which is usually divided by sections. It is the investigating CI special agent's file and frequently the most complete of the duplicative copies of the case file maintained at the various levels of oversight and command. It contains the original signature copies of IMFRs, statements, and other evidentiary documents. A well-organized field file is the foundation of a strong case. While field dossiers will be established based upon ATCICA requirements and unit SOPs, the following is the general content of most dossiers.

2-176. The most critical document in terms of continuity of investigative effort and institutional memory of an investigation is the agent's log. The log is maintained on a DA Form 1594 (Daily Staff Journal or Duty Officer's Log), or electronic equivalent, and is filed in the front of Section 2 of the field dossier. It can be either handwritten or typed, and is often maintained in softcopy and printed and placed into the field dossier periodically.

2-177. The first entry in the log is the case opening message that opened the case. Everything is entered into the Agent's log as it is entered into the field dossier, the CI incident report, IMFRs, ATCICA administrative memorandums, tasking memorandums, MFRs, conversation records, important emails, summary of briefings, legal and intelligence oversight reviews, and other relevant documents. Additionally, important actions that should be documented but do not generate a report should be annotated; for example, supervisory case reviews. All numbers on the log should be consecutive starting with # 1. On each document in the lower right corner, write in pencil the log number which corresponds to the log entry. Each incident should be annotated on DA Form 1594 as follows:

- **Section 1—CI incident report.** File a copy of the CI incident report or any other documentation which was used as predication for opening the case. The other documentation could be an FBI letterhead memorandum (LHM), poly report referral from ACICA, memorandum from ACICA, request from DSS, or other directive memorandum. Copies of all the IMFR should be kept in this area in reverse chronological order. In this section put the LHM requesting a joint investigation if applicable.
- **Section 2—ATCICA and ACICA administrative messages.** File all administrative memorandums that are sent to the field. All tasking memorandums to the field concerning this case are filed here in reverse chronological order. Place DA Form 1594 (on which every action is logged) on top of this section to maintain a chronological listing of significant case activity, both administrative and investigative.
- **Section 3—planning documents and outstanding requests.** File all IPs, SIPs, and lateral leads to other field offices requested by the investigating CI special agents in this section, as well as lateral leads and requests for NACs concerning this investigation. Also file all emails requesting extensions on the suspense and discussions on the case, procedure requests, and administrative memorandums from the field.
- **Section 4—investigative memorandums for record.** File copies of all IMFRs in reverse chronological order. FBI FD-302 forms, which are used to report or summarize interviews conducted, are considered the equivalent of IMFRs in joint investigations. (In joint investigations with any other service or agency, any report written by the other service is considered equivalent to an IMFR.)
- **Section 5—MISC.** File fully filled-out conversation records, ACIC analysis reports, investigating CI special agent's analysis, and miscellaneous emails in reverse chronological order. An investigative memorandum for record will be used to record verbal coordination pertinent to the investigation.

- **Section 6—original signature documents.** Place original signature documents in this section immediately upon creation. Copies of any original signature documents should be made and put in section 4. Field elements will retain original documents of all reports and exhibits in a field case file throughout the duration of the investigation. Original reports and exhibits will not be destroyed, defaced, or mutilated.

Counterintelligence Incident Report

2-178. The CI incident report, usually generated by a walk-in source, is forwarded through the ATCICA to the ACICA for a determination on whether or not to open an investigation. Copies of all CI incident reports will be retained by the investigating element in accordance with AR 25-400-2 until destruction is authorized and/or in accordance with unit SOPs.

Investigative Memorandum for Record

2-179. The investigative memorandum for record (IMFR) records information obtained because of various investigative activities, including source interviews, others knowledgeable interviews, subject interviews, and records checks. The CI special agent likewise prepares the IMFR and forwards it through channels to the appropriate ATCICA. An IMFR is produced after each completed investigative activity and forwarded to the ATCICA. Copies of all IMFRs will be retained by the investigating element until the investigation is completed and maintained on file in accordance with AR 25-400-2 until destruction is authorized and/or in accordance with unit SOPs.

Report of Investigation

2-180. The ROI serves as an executive summary of investigative results reported in IMFRs and exhibits. ROIs are required for any investigation that goes beyond the interviews of the original sources of information and local and military agency checks. The ROI highlights investigative efforts to either confirm or refute espionage indicators or allegations. The report should be concise, ensuring pertinent results are emphasized. The agent preparing the ROI cites investigative findings to explain, refute, or support allegations or incidents in which espionage activity is suspected. Copies of all ROIs will be retained by the investigating element until the investigation is completed and maintained on file in accordance with AR 25-400-2 until destruction is authorized and/or in accordance with unit SOPs.

Summary of Information

2-181. The SOI is a formal method of providing information to agencies and elements outside Army intelligence investigative channels. The agencies may include local and national level agencies, as well as unit commanders or LEAs. Typically, the SOI is used to provide information to the agency or organization that has primary jurisdiction and responsibility for responding to the incident. The SOI provides a summary of the referred incident and the results of any Army intelligence investigative activities. As examples, upon case termination, the ATCICA may task the lead agent to pass an SOI to the FBI for further investigation; or to a unit commander for further inquiry or action under the UCMJ. This chapter is intended to provide a standardized format and basic guidance for the preparation, passage, and tracking of the SOI. Once Army intelligence passes an SOI to the responsible agency or element, it must follow-up and determine what actions were taken as the result of the SOI's passage. The result must be reported to the responsible ATCICA via an administrative message, as soon as available.

Letter of Transmittal

2-182. The first part of the SOI consists of a transmittal memorandum. This memorandum is prepared on letterhead stationery and conforms to the guidance in AR 25-50. There are two different versions depending on if the agency receiving the SOI is within the military or a non-DOD agency. This transmittal memorandum is used to briefly explain the circumstances surrounding the acquisition of the information, reason for providing the information to the addressee, and Army intelligence concerns and desires.

2-183. The transmittal memorandum may be classified or unclassified, depending upon content, although agents should try to keep the transmittal memorandum unclassified. The transmittal memorandum provides all professional administrative information, comments, and recommendations, which does not belong in the SOI itself. Case control numbers should not be provided in the covering memorandum nor is it necessary to provide or cross-reference actual case titles. The SOI transmittal memorandum will be signed by the senior CI special agent.

Actual Summary of Information

2-184. The SOI is prepared on plain bond paper and is unsigned. The SOI summarizes the information reported and developed by Army intelligence. The ASCCN or LCCN will be positioned directly below the subject line, in the same format as IMFRs. It is not necessary to specifically identify sources of information unless it is anticipated that the receiving agency of the SOI will need to contact or further question the original Army intelligence sources.

Note. This is why it is important when interviewing a source to cover the four basic points of the Privacy Act of 1974, with emphasis that such information or identification may be provided, as necessary, to other responsible agencies.

Privacy Act of 1974

2-185. This advisement shows that subjects and sources understand their rights under the Privacy Act and the voluntary nature of furnishing any personal information to special agents. The Privacy Act statement is maintained in the local case file and is NOT forwarded as an exhibit to be archived with the ROI. There is no regulatory requirement to advise non-U.S. persons of the provisions of this act. Privacy Act advisements are not required in interviews with foreign nationals in overseas areas. The investigating element will retain copies of all Privacy Act statements until the investigation is completed; they will be maintained on file in accordance with AR 25-400-2 until destruction is authorized and/or in accordance with unit SOPs.

Sworn Statement

2-186. The sworn statement is a primary evidentiary document within the investigative case file. It records a voluntary statement made by a source, subject, or accused, under oath or affirmation. When properly completed, it is a legal document and lends credibility to any information furnished. The sworn statement is attached to the IMFR as an exhibit and is unaltered from when the subject, source, or accused wrote it. The sworn statement is filed with the IMFR as an exhibit. It is usually unclassified, unless the subject or source puts classified information into it. The investigating element will retain copies of all DA Forms 2823 until the investigation is completed; they will be maintained on file in accordance with AR 25-400-2 until destruction is authorized and/or in accordance with unit SOPs.

Rights Warning

2-187. DA Form 3881 records the fact that a U.S. person was advised of individual rights under the Fifth Amendment to the U.S. Constitution, or rights under Article 31, UCMJ. It is used when questioning a suspected or accused individual concerning a criminal act or national security crime of which they are suspected or accused. This form is also used for military subjects who incriminate themselves during interviews or for military subjects and accused persons who are interviewed or are asked to provide information of a possibly incriminating nature. It further records the individual decision to exercise or waive those rights. When used, it is attached to the IMFR as an exhibit.

2-188. Procedures for advising a person of their legal rights are fully explained on the reverse side of DA Form 3881. The investigating element will retain copies of all DA Forms 3881 until the investigation is completed and maintained on file in accordance with AR 25-400-2 until destruction is authorized and/or in accordance with unit SOPs.

Secrecy Affirmations

2-189. This affirmation shows that a source or subject who is involved in some form of CI activity understands that disclosure of the nature or existence of the activity is prohibited without the express approval of Army intelligence. The Secrecy Affirmation is maintained in the local case file and is NOT forwarded as an exhibit to be archived with the ROI. The investigating element will retain copies of all secrecy affirmations until the investigation is completed and maintained on file in accordance with AR 25-400-2 until destruction is authorized and/or in accordance with unit SOPs.

Exhibits Cover Sheets

2-190. Exhibits are documentation or physical evidentiary materials which support the information provided in an IMFR. This evidence may be in the form of records, such as identification documents, affidavits, statements, photographs, transcripts of interviews, photo copies, sketches (made by either the special agent or other persons), pamphlets, newspaper clippings, sound recordings, surveillance logs, DA Forms 4137 (Evidence/Property Custody Document) and 2823, computer memory devices, or transcripts concerning the analysis of information storage medium.

2-191. Exhibits augment and support, but do not replace the IMFR. An exhibit cover sheet is used to identify exhibits, usually documents, collected during the course of an investigative activity. This cover sheet identifies the specific investigation to which the exhibit relates, control number, date of related IMFR, and a description of the exhibit.

2-192. Special agents will provide a copy, or reasonable description, of all exhibits to the ATCICA when the IMFR is submitted. If the investigative activity was conducted as an RFA, a copy of the exhibit will be retained in the field case file of the investigating unit; the original IMFR and exhibit, with the exhibit cover sheet, will be sent to the ATCICA. Investigating CI special agents will maintain the original copy of all exhibits other than RFAs, which will be maintained at ATCICA for inclusion in the ROI, when ATCICA terminates the case.

2-193. Exhibit cover sheets are transmitted with the exhibit and the IMFR reporting the results of investigative activity in which the exhibit material was collected. Exhibit Cover sheets are maintained in the local case file, along with the corresponding exhibit. The investigating element will retain copies of all exhibits until the investigation is completed and maintained on file in accordance with AR 25-400-2 until destruction is authorized and/or in accordance with unit SOPs.

Requests for Assistance

2-194. RFAs, lateral leads, and call spy hotline taskings are all requests for assistance documents. Field elements will file case material relating to lateral leads originating from another theater ATCICA, Federal LEAs, HN CI or police agency, or a sister service, in the appropriate investigative case folder. Original reports and exhibits will be forwarded to the lead agent or appropriate ATCICA within five work days after completion of tasking, or as directed by ATCICA.

2-195. Field elements will confirm receipt of all original copy case material from the field element or ATCICA generating the request. Each field office will maintain a file containing all taskings from the ATCICA, requests from other agencies, and any IMFRs, MFRs, or CI incident reports written to support these taskings. Before destroying these files ensure all original signature documents not originating at the ATCICA have been transmitted to the ATCICA. Copies of original signature investigative documents and supporting documentation will be retained for one year from last action. If the field element desires to retain the file, a retention determination will be sought from the responsible unit intelligence oversight officer.

This page intentionally left blank.

Chapter 3

Counterintelligence Operations

Army CI supports full spectrum operations. CI elements focus on and dedicate their efforts to detecting, identifying, neutralizing, and/or exploiting adversary intelligence elements attempts to collect information on U.S. forces. CI is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements of foreign organizations, persons, or international terrorist activities.

GENERAL

3-1. CI operations are activities designed to detect, identify, assess, counter, exploit, and/or neutralize the intelligence collection activities of FISS and ITO entities targeting Army equities. The objective for all CI operations is to disrupt or deny FISS and ITO targeting; provide support to specific Army programs; or CI support to various types of military operations. CI operations generally use a combination of the core CI functions (investigations, collection, analysis and production, and technical services and support) to reach the objective.

3-2. However, all core CI functions are mutually supporting and one function may transition to or initiate one or more of the other functions. For example, an on-going collection activity may reveal a possible CI incident which requires the conduct of a CI investigation; or during the analysis of compiled CI information a potential lead may be identified who may be used as a source to gather information on local insurgent collection activities. CI operations can be either offensive or defensive in nature and generally use investigative and/or collection activities to fulfill the object of the program. Figure 3-1 (page 3-2) shows types of CI operations. CI operations fall into two categories:

- **Counterintelligence sensitive operations.** Proactive and targeted activities that involve direct or indirect operations against a known or suspected FISS and ITO threat. Offensive CI operations are governed by AR 381-47 (S). Refer to this manual for detailed information concerning CI projects, investigative source operations, defensive source operations (DSO), and CFSO.
- **Counterintelligence support operations.** DSO and offensive CI operations (OFCO) support Army operations, force and technology protection, security projects, and information programs. These programs are aimed at supporting the protection programs and formal security programs of Army commanders at all levels.

ADVICE AND ASSISTANCE PROGRAMS

3-3. Advice and assistance programs are conducted by CI teams at all levels to improve the security posture of supported organizations. These programs aid security managers in developing, sustaining, or improving security plans and SOPs. Advice and assistance can help identify and neutralize threats to security from FISS and ITO who attempt to obtain information about U.S. forces, programs, and operations. These programs provide threat information and identify specific vulnerabilities to security beyond the capability of a security manager. Advice and assistance can include but is not limited to—

- Conduct of inspections, security planning, resolution of security problems, or development of classification guides.
- CI surveys, technical inspections, and preconstruction technical assistance.

- Training, providing CI materials, and training security managers on CI programs.

COVERING AGENT PROGRAM

3-4. CI CAP support is the technique of assigning a primary supporting CI special agent to a command or agency. This agent will conduct all routine liaisons and provide advice and assistance with the supported element. It ensures detailed familiarity with the supported element's operations, personnel, security, and vulnerabilities, and in turn provides the element with a POC for reporting matters of actual or potential CI interest. The CAP also allows the CI special agent to provide services that are tailored to the individual organization's mission.

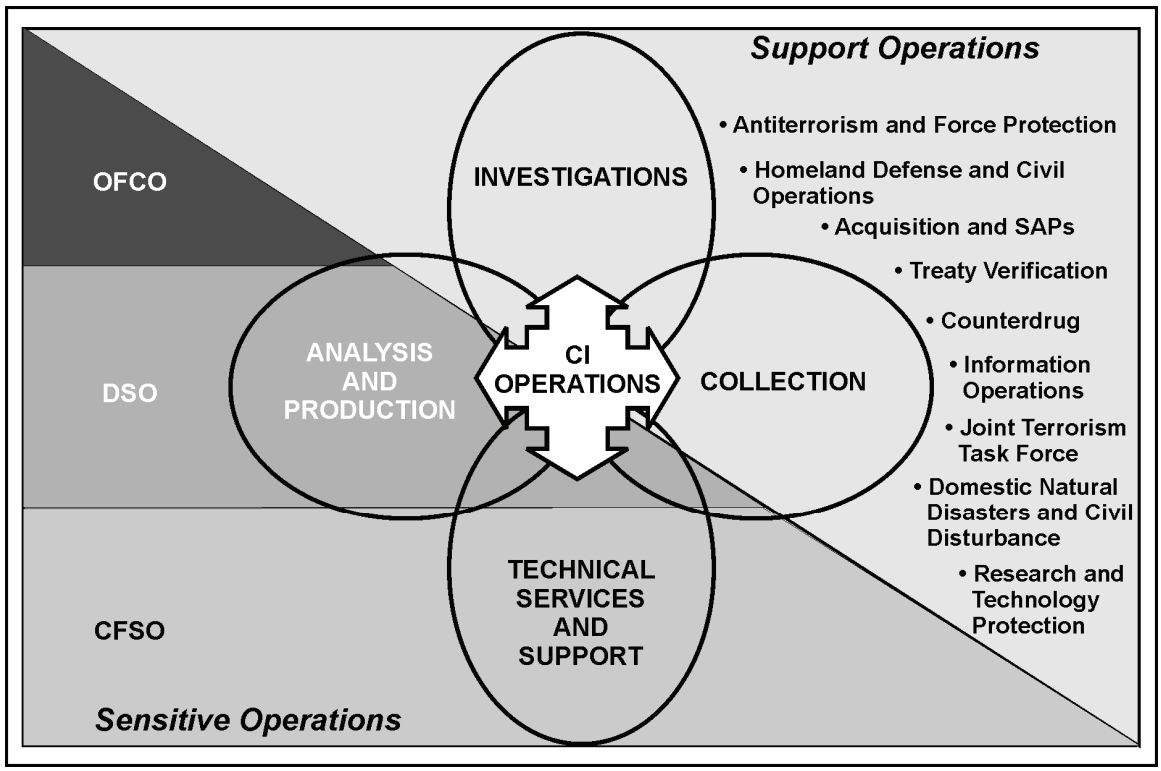

Figure 3-1. Counterintelligence operations

COUNTERINTELLIGENCE SUPPORT TO RESEARCH AND TECHNOLOGY PROTECTION

3-5. CI support to research and technology protection (RTP) prevents the illegal diversion or loss of DOD critical technology. RTP entails identifying, assessing, and developing countermeasures to FISS and ITO targeting, exploitation, or the illegal diversion of Army and associated DOD technologies, systems, and components. CI support to RTP utilizes the full range of CI activities, to support and protect critical program information. CI support to RTP will span the entire life of the program, from concept, through development and fielding, to expiration of the technology or system. The Army G-2X is the program manager for CI support to RTP in the Army. CI support to RTP includes—

- Providing FISS and ITO threat information and analysis to all personnel and agencies associated with an RTP program.
- Providing support to TAs and VAs for an RTP.
- Identifying and developing countermeasures to protect the supported program.

- Providing tailored threat awareness briefings to program personnel.
- Debriefing program personnel who have been in contact with representatives of foreign governments, international organizations or other foreign contractors, or attending symposiums or trade shows which may have brought them in contact with potential FISS and ITO collectors.
- Conducting joint investigations with other security or LEAs supporting the program to prevent the loss of technology or compromise of the program.
- Conducting damage assessments of programs that have potentially been compromised.
- Developing a tailored counterintelligence support plan (CISP) for the supported program.

COUNTERINTELLIGENCE SUPPORT TO ACQUISITION AND SPECIAL ACCESS PROGRAMS

3-6. Army CI provides support to research, development, technology, and evaluation (RDT&E); acquisition elements through the Acquisition System Protection Program to prevent the illegal diversion or loss of critical military and defense technology. Acquisition systems protection integrates all security disciplines, CI, and other defensive methods to deny FISS and ITO collection efforts and prevent unauthorized disclosure to deliver our forces uncompromised combat effectiveness over the life of the system. CI support is provided to protect U.S. technology throughout the acquisition process.

3-7. SAPs usually involve military acquisition, intelligence, and operations and support activities. When applicable, CI support to SAPs extends to government and industrial security enhancement; DOD contractors and their facilities in coordination with DSS as appropriate; and the full range of RDT&E activities; military operations; and intelligence activities for which DA is the proponent or the DOD executive agent. INSCOM is responsible for providing the life cycle support and maintaining the capability, experienced personnel, and resources for CI support to SAPs. For more information on SAPs see AR 380-381.

3-8. The CI support plan (CISP) is a formal agreement between the supporting CI element and the supported program manager. The CISP identifies the roles, resources, and activities that Army CI will provide to the supported program as well as all coordination with program elements or other agencies involved with the program. The CISP should be reviewed annually and changes should be made whenever there are significant changes to the program. All CISPs will be reviewed by the Army G-2X or ACICA. There are two types of CISPs:

- **Program.** Programs that develop critical program information.
- **Facility.** Any facility used for research and development associated with critical program information.

COUNTERINTELLIGENCE RED TEAM OPERATIONS

3-9. Upon request by a commander or program manager, CI personnel may plan and execute a simulation of FISS and ITO targeting, such as an installation, operation, or program. Such simulations are informally known as red team operations. Red team operations identify weaknesses in systemic or security programs that could be exploited by FISS and ITO. Upon completion of a red team operation, a formal assessment will be given to the commander that also includes countermeasures and/or recommendations to overcome, reduce, or mitigate vulnerabilities. There is no single structure or composition for a red team. Red team operations include, but are not limited to, the following:

- **Open-source collection.** Often open-source collection will help the red team establish a profile of the unit or agency as well as key personnel and to formulate a collection plan.
- **"Dumpster diving."** This is a search of unit trash which can provide details on past, present, and future mission activities, biographic data on assigned personnel, and unit structure.

- **Elicitation.** This involves conducting elicitation among target personnel where they socialize or congregate to obtain information on the target unit or organizations mission, capabilities, or plans.
- **Technical collection.** This operation includes COMSEC monitoring, electronic, and/or technical surveillance with the approval of the commander or program manager, and the approvals required by AR 380-53 and AR 381-10.

3-10. Because of the complexity and high resource requirements, red team operations generally should be limited to extremely sensitive activities, such as SAPs and RTPs, although red team operations may be useful with major tactical exercises and military operations. Commanders must ensure compliance with laws, policy, and regulations when employing technical collection techniques to support red team operations. All red team operations will be approved by the CICA before execution.

COUNTERINTELLIGENCE SUPPORT TO TREATY VERIFICATION

3-11. A security consequence of arms control is an overt presence of FISS and ITO at U.S. facilities. CI is concerned with non-treaty related activities of foreign visits to Army installations and protecting installation activities not subject to treaty verification. CI personnel provide advice and assistance to installation commanders and debrief personnel who may have come in contact with inspectors. The Defense Threat Reduction Agency has overall responsibility for CI support to treaty verification. INSCOM, with Army Forces Command support, is responsible for treaty verification support within CONUS. ASCC and combatant command CI elements are responsible for treaty verification that affects unified, Army component, or allied commands.

COUNTERINTELLIGENCE SUPPORT TO ANTITERRORISM AND PROTECTION

3-12. Title 50, USC § 401a, implemented the National Security Act of 1947. It defines CI as "information gathered, and activities conducted, to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities." Army CI is responsible for identifying terrorist indications and warning (I&W) to Army equities; however, countering and neutralizing terrorist activities is a multi-agency task under the Army's antiterrorism (AT) program (AR 525-13). (See also AR 381-20, chapter 9.)

3-13. Terrorism is defined as the calculated use of unlawful violence or threat of unlawful violence to instill fear that is intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Combating terrorism has two major subcomponents: AT and counterterrorism (CT). As defined by DOD—

- Antiterrorism are those defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces.
- Counterterrorism are those operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism.

3-14. Army CI is a key contributor in preventing and deterring terrorist activities targeting Army and DOD interests. Army CI supports the AT program through the execution of all the CI functions (investigations, collection, analysis and production, and technical services and support). Army CI generally focuses on the FISS and ITO intelligence collection and targeting activities directed at Army equities to provide I&W of exploitation or potential attacks. Unless assigned to a CT unit, Army CI is continually engaged in an AT role to help detect and identify FISS and ITO collection threats and terrorism I&W. AR 525-13 stipulates that the Army will—

- Conduct foreign intelligence collection and CI activities to collect and disseminate information on foreign threats against the Army.
- Sustain an intelligence capability to monitor and report on the activities, intentions, and capabilities of FISS and ITO and other foreign threat groups in accordance with applicable regulations and directives.
- Maintain a capability to report and disseminate, time-sensitive information concerning the foreign threat against Army personnel, facilities, and other assets.
- Provide supported Army commanders with information concerning the foreign threat against their personnel, facilities, and operations consistent with the provisions and limitations of AR 381-10 and other applicable regulations and directives.
- Include foreign threat information in briefings on CI in accordance with AR 381-12.
- Serve as the Army intelligence liaison representative to Federal, state, and local agencies and host country Federal, state, and local-level agencies to exchange foreign threat information.

3-15. The role of CI is to support the commander's requirements to preserve essential secrecy and to protect the force directly or indirectly. To be most effective, CI should be thoroughly integrated into the commander's operational planning and preparation. The CI mission makes it an ever-present AT enabler through the routine execution of its functions. However, CI can tailor its functions to provide support to AT and protection specific operations including—

- Screening LEPs working on OCONUS military installations.
- Tailoring security education and awareness briefings and programs.
- Conducting travel and foreign contact briefings and debriefing programs.
- Supporting TAs and VAs.
- Providing FISS and ITO threat analysis and products.
- Conducting CI investigations and collection that impact AT and protection.

THREAT ASSESSMENTS AND VULNERABILITY ASSESSMENTS

3-16. AR 525-13 requires commanders, down to battalion level, to appoint an AT officer who serves as his advisor on all AT matters. The AT officer is the catalyst for implementing the AT program within the unit. The AT officer is responsible for obtaining support to the unit's AT program to include scheduling and coordinating VAs to assess the unit's protection postures. VAs are conducted by multiple agencies with differing areas of subject matter expertise including—

- Physical security.
- Explosive ordnance disposal.
- Engineering.
- CI.
- Information management.
- Law enforcement.
- Medical.

3-17. While Army CI has been synonymous with the term "force protection" for many years, protection is an Army program and a commander's responsibility. AR 525-13 provides guidance to unit and installation commanders to conduct VAs to identify weaknesses in security and protection posture and to provide countermeasures recommendations.

3-18. The unit AT and protection officer is the focal point for coordinating and obtaining support for the conduct of VAs on critical facilities, operations, and infrastructure within their unit. The focus of VAs is to determine the unit's ability to protect personnel, information, and critical resources by detecting or deterring threat attacks and failing that, to protect by delaying or defending against threat attacks.

3-19. Additionally, these assessments will verify compliance with applicable Army and combatant command standards. CI support to the conduct of AT and protection VAs consists of producing a TA and making countermeasures recommendations in the final VA report concerning specific areas related to countering or negating known or suspected collection targeting of the supported command.

3-20. TAs are products focused on the leadership, structure, capability, methods of operations, targeting focus, and activities of known or suspected FISS and ITO for a specific area or location. A TA is a stand-alone document. TAs are produced from existing intelligence analysis as well as information developed through all CI functions and liaison with other security, intelligence, and LEAs.

3-21. A VA is a detailed assessment for a specific target; unit, facility, mission-essential vulnerable area (MEVA), C2 nodes, installation, activities, or operation. The role of CI to support a VA should be threat based. Some questions to consider are—

- What groups are targeting personnel and equipment?
- What methods are these groups using to gain access to the post?
- How are they collecting information?
- What do they already know about our operations?

3-22. The CI focus in a VA is not only on the known, suspected, or potential FISS and ITO threat to the target but also on weaknesses in systemic procedures that could be exploited by FISS and ITO to collect on the target and potentially exploit or attack the target. The VA should also include CI countermeasures recommendations to the commander on how to neutralize, reduce, or mitigate those vulnerabilities to enhance the target's posture and minimize threats to his personnel, facilities, and operations. Specific areas of CI interest in VAs are—

- **Physical security.** Physical barriers, access controls, guard force procedures and how they can be penetrated or bypassed by FISS and ITO operatives.
- **Personnel security.** Access to classified or restricted areas, clearance procedures to mitigate the ability of a FISS and ITO operative to remove information or coerce someone with placement and access to remove information from an installation or facility.
- **Information security.** Document handling, storage, and destruction.
- **Information systems security and telecommunications security.** Vulnerabilities to the systems and susceptibility to intercept or compromise by a FISS and ITO threat.
- **OPSEC.** Signatures, patterns, movement, or activities that can provide an indication of plans, intentions, or capabilities.

COUNTERINTELLIGENCE SUPPORT TO HOMELAND DEFENSE AND CIVIL SUPPORT OPERATIONS

3-23. Under the provisions of the Posse Comitatus Act, Federal U.S. military forces are restricted from assisting in policing or law enforcement activities except when authorized to do so. Because Army CI authority is narrowly focused, the role of CI in domestic operations is very limited. Generally, the role of CI is limited to—

- Conducting liaison with local, state, and federal security, intelligence, and LEAs.
- Providing FISS and ITO threat and vulnerability analysis to the supported military unit.

- Sharing information between DOD and the supported unit or agency.

3-24. During national disaster and civil disturbances, the potential collection threat to Army equities is remote. During these types of operations, CI is strictly limited to conducting liaison between civilian LEAs and the supporting military unit to obtain any protection information that could affect the ability of the supporting military unit to effectively execute its mission.

COUNTERINTELLIGENCE SUPPORT TO JOINT TERRORISM TASK FORCE

3-25. The JTTF program was established in September 2001. The JTTF is a task organization of multiple different law enforcement, security, intelligence, and defense agencies to detect, identify, and counter terrorist activities against U.S. interests. Army CI is an active participant in the JTTF program. The role of Army CI includes—

- Providing FISS and ITO threat analysis.
- Identifying any FISS and ITO threat information that may impact Army equities.
- Conducting or supporting joint investigations with other national agencies, with the appropriate approval, which may affect Army equities.

COUNTERINTELLIGENCE SUPPORT TO COUNTERDRUG OPERATIONS

3-26. The military participates in counterdrug operations under the provisions of the National Drug Control Strategy. Military forces may be employed in a variety of operations to support other agencies responsible for detecting, disrupting, interdicting, and destroying illegal drugs and the infrastructure (personnel, material, and distribution systems) of illicit drug trafficking entities. Military counterdrug efforts support and complement rather than replace counterdrug efforts of Federal, state, and local LEAs in cooperation with foreign governments. CI support to counterdrug operations is generally restricted to—

- Conducting liaison with local, state, and Federal security, intelligence, and LEAs.
- Providing threat and vulnerability analysis of international drug organizations that threaten the security of U.S. forces.

COUNTERINTELLIGENCE SUPPORT TO INFORMATION SUPERIORITY

3-27. Information superiority is an evolving concept and operational strategy within the context of Army operations. As a result, Army doctrine will continue to change to reflect changes in TTP, operational focus, and execution. Existing information superiority doctrine identifies CI as a core supporting element of the information tasks conducted to protect U.S. forces networks while simultaneously degrading the adversary's networks and decisionmaking process. Information superiority is an integrating strategy that incorporates several existing DOD missions within a theater of operations to ensure U.S. commanders obtain information superiority over their adversaries. These tasks are designed to protect our information, information systems, and decisionmaking process (offensive tasks), ultimately resulting in U.S. information superiority. Information superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

3-28. The information tasks identified in FM 3-0 are information engagement, C2 warfare, information protection, OPSEC, and military deception. CI is specifically identified as a capability that can support these tasks. CI support is essential to the execution of the information tasks at all echelons (tactical, operations and strategic). Although FM 3-0 only identifies CI as a capability that supports the OPSEC task,

CI can support all the information tasks using one or more of the CI functions of investigations, collection, analysis and production, and technical services and support. Figure 3-2 shows the CI support to Army information tasks.

3-29. CI is instrumental in collecting and analyzing information about the adversary's intelligence assets, capabilities, processes, and intent that can affect U.S. information superiority. CI can provide the commander with the understanding of what the FISS and ITO collects and believes. This allows operational planners to tailor information tasks to manipulate the adversary decisionmaking process and affect the outcome of future adversary actions.

Task	*Information Engagement*	*Command and Control Warfare*	*Information Protection*	*Operations Security*	*Military Deception*
Intended Effects	• Inform and educate internal and external publics • Influence the behavior of target audiences	• Degrade, disrupt, destroy, and exploit enemy C2	• Protect friendly computer networks and communication means	• Deny vital intelligence on friendly forces to hostile collection	• Confuse enemy decision makers
Capabilities	• Leader and Soldier engagement • Public Affairs • PSYOP • Combat camera • Strategic communication and Defense Support to Public Diplomacy	• Physical attack • Electronic attack • Electronic warfare support • Computer network attack • Computer network exploitation	• Information assurance • Computer network defense • Electronic protection	• OPSEC • Physical security • **Counter-intelligence**	• MILDEC
Counter-intelligence Support	• **Provide analysis to identify target audiences to maximize perception management and theme dissemination**	• **Collect information for targeting and neutralization of CI targets to affect the adversaries' visualization and knowledge of US plans, intentions, and capabilities**	• **Conduct TA and VA to identify vulnerabilities and recommend countermeasures** • **Conduct CI investigations**	• **Conduct SAEDA, terrorism, and FP briefings to raise awareness and educate personnel on reporting responsibilities** • **Conduct TA and VA**	• **Conduct analysis to identify AFIST collection and targeting to support MILDEC planning** • **Collect information to determine if MILDEC activities have been compromised**

Figure 3-2. Counterintelligence support to Army information tasks

COUNTERINTELLIGENCE SUPPORT TO MILITARY DECEPTION

3-30. Military deception comprises those actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations; this causes the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. CI support to military deception is designed to deliberately neutralize, degrade, mislead, or manipulate adversary intelligence services. CI support to military deception assists in identifying an adversary's intelligence services; for example:

- Assessment of U.S. capabilities, intentions, operations or likely COAs.
- Susceptibility to U.S. military deception.

- Capability to detect deception.
- Conduits in which military deception information may be passed.
- Collection assets and capabilities that may be targeting U.S. military deception plans.

3-31. This information can be collected through CI source operations, CI investigations, CI debriefings of DOD personnel, and CI screenings of local national workers and contract linguists. Information of this type collected from detainees is of CI interest and should be channeled as such. CI threat analysis (CITA) can help determine if the adversary is susceptible to or have indicators of our military deception operations.

COUNTERINTELLIGENCE SUPPORT TO PSYCHOLOGICAL OPERATIONS

3-32. PSYOP are planned operations that convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately to influence the behavior of foreign governments, organizations, groups, or individuals to support U.S. national objectives. CI support to PSYOP consists of countering adversarial HUMINT targeting of U.S. PSYOP and providing CITA for counter-SIGINT analysis pertinent to PSYOP. Information provided by CI can assist the commander and staff in developing a U.S. PSYOP strategy with the ability to counter, deter, neutralize, exploit, or at least mitigate the adversary's PSYOP program.

3-33. The first message presented to the general population is often the one that is perceived to be the most truthful and consequently the one that bears more credence. Imagine an adversary gaining access to our PSYOP message before its release and preempting that message with one of their own. The successful execution of PSYOP requires CI to be knowledgeable of the adversary's intelligence collection threat and their intent to collect against friendly PSYOP. CI products pertinent to PSYOP planning include current CI reporting, CI estimates, and country studies.

3-34. CI assets at all echelons should continually be provided with information about specified PSYOP missions to ensure CI investigations, local national and contract linguist screenings, collection, targeting, and products that support PSYOP remain current. CI assets not only answer the interrogatives concerning adversarial intelligence targeting of a U.S. PSYOP operation but also may be able to provide feedback about threat reactions to U.S. PSYOP messages to ascertain the effectiveness of the U.S. PSYOP mission.

COUNTERINTELLIGENCE SUPPORT TO ELECTRONIC WARFARE

3-35. *Electronic warfare* (EW) is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-13.1). The three major components of EW are electronic protection (EP), electronic warfare support (ES), and electronic attack (EA). CI provides support to EW via its inherent collection of information about the adversary EW program and their intent to direct their EW assets against U.S. forces SIGINT vulnerabilities and communications security complacency.

3-36. Source operations can collect information on the adversary's EW plans and their use of the electromagnetic spectrum including the targeting of U.S. SIGINT. CI collection can also determine what knowledge adversary intelligence has of U.S. forces SIGINT vulnerabilities and any complacency shown on the part of U.S. personnel in regards to COMSEC measures.

3-37. CI threat analysts can use that information and analytical techniques and procedures to develop an electronic summary of the battlefield, which can assist decisionmakers in developing the U.S. forces EW plan. CITA during EW planning consists of a 5-step process: development of a database, a threat assessment, a vulnerability assessment, countermeasures options development, and countermeasures evaluation.

COUNTERINTELLIGENCE SUPPORT TO OPERATIONS SECURITY

3-38. OPSEC denies the enemy the information needed to correctly assess friendly capabilities, plans, or intentions. OPSEC is a process beginning with identifying essential elements of friendly information (EEFIs) or critical information and analyzing friendly actions attendant to military operations and other activities. The results of that analysis is used to identify those actions or indicators that can be observed by adversary intelligence that could be interpreted or pieced together to derive EEFIs for use by adversaries.

3-39. The next step is to select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. The five actions involved in the OPSEC process are—

- Identifying EEFIs or critical information.
- Analyzing the adversary.
- Analyzing U.S. vulnerabilities.
- Assessing risk.
- Applying appropriate OPSEC measures.

3-40. CI support to OPSEC entails identifying adversary intelligence, TTP, collection methods, analysis, and exploitation capabilities that target our EEFIs, and then developing countermeasures.

3-41. CI investigations, CI source operations, debriefing of DOD personnel, and screenings of local nationals and contract linguists can determine what EEFIs are being targeted by foreign intelligence and what adversary collection methods and capabilities are being utilized to collect EEFIs. Additionally, cyber CI elements can perform Internet open-source collection and DOD network and systems analysis to determine OPSEC vulnerabilities and provide support to the conduct of Army network threat and VAs. The information provided by CI will aid the OPSEC planners in identifying and protecting EEFIs, identifying OPSEC indicators, and developing OPSEC measures.

3-42. In accordance with AR 530-1, the Commander, INSCOM, will provide data on the foreign intelligence threat, terrorist threat, and CI support to OPSEC programs for Army units, ASCCs, direct reporting units, and above. The INSCOM elements will provide information updates, but will not write threat assessments for the supported command or agency. (The supported organization's intelligence staff element performs this function.) Due to changes in AR 530-1, CI support to OPSEC at echelons above corps and echelons corps and below will occur as resources permit. CI may also provide threat briefings and training concerning the protection of U.S. classified information.

COUNTERINTELLIGENCE SUPPORT TO COUNTERPROPAGANDA

3-43. Propaganda is any form of communication to support national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group to benefit the sponsor, either directly or indirectly. It is normally directed at the U.S., multinational partners, and key audiences in the AO. Propaganda operations are deliberately designed to attack the will of nations to resist and Soldiers to fight. Propagandists seek to mix truth and lies in a way that listeners cannot detect.

3-44. Counterpropaganda operations are structured to detect and counter adversary attempts to convey selected messages to U.S. and allied audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of governments, organizations, groups, and individuals. Counterpropaganda operations identify adversary propaganda, contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces.

3-45. CI supports counterpropaganda efforts by providing planners with information regarding adversary propaganda operations. It is possible CI elements may learn of an adversary's impending propaganda message before the adversary's release of that information. This would provide DOD with a chance to preempt their message with one of our own. CI identifies adversary propaganda efforts through CI source operations, CI investigations, and local employee and contract linguist CI screenings.

COUNTERINTELLIGENCE SUPPORT TO COUNTERDECEPTION

3-46. The objectives of counterdeception are to negate, neutralize, and diminish the effects of or gain an advantage from an adversary's deception operation. Knowing what deception methods an adversary has used in the past is important. Equally important is properly considering tactical indicators and not dismiss them because they conflict with preconceptions. Dismissing them will enable an adversary's deception that plays on those preconceptions to succeed.

3-47. CI analysis provides awareness of an adversary's posture or intent and identifies an adversary's attempt to deceive friendly forces. An adversary's intelligence collection priority can provide indicators for their actual collection requirements and also for deception planning and operations. Not only is it necessary to uncover the adversary's deception plan but also it is equally important to not allow the adversary to know we have uncovered their deception plan.

3-48. CI source and screening operations can identify adversary CI and HUMINT operations and ISR capabilities attempting to find out what we know of their deception plan. The CITA cell can analyze information we have on the adversary deception plan and provide support to counterdeception.

COUNTERINTELLIGENCE SUPPORT TO PHYSICAL SECURITY

3-49. Physical security is that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

3-50. CI support to physical security provides an additional line of defense in a physical security and AT program through the use of CI source operations, CI screenings, debriefing of DOD personnel, and CI investigations. CI supports the safeguarding of personnel and the prevention of unauthorized access to equipment, installation, material, and documents by producing a well-planned, systematic CISP that clearly identifies the threat. Additionally, CI analysis provides I&W of potential terrorist attacks and information for proactive CT operations. CI investigations reveal attempts by foreign intelligence entities to use espionage and sabotage to target U.S. forces.

3-51. Effective CI support to physical security provides decisionmakers with information and timely warnings of adversary intelligence operations, planning being based on those operations, and likely adversary COAs targeting DOD assets.

COUNTERINTELLIGENCE SUPPORT TO PHYSICAL DESTRUCTION

3-52. Physical destruction is the application of combat power to destroy or degrade adversary sources of information and C2 systems. Effective physical destruction also damages the adversary's ability to collect, analyze, retain, and disseminate information. Physical components of the information infrastructure and supporting functions, such as electric power, communications links, and human operators, are likely targets. Physical destruction includes direct and indirect fires from ground, sea, and air forces, and may include both lethal weapons (bullets and bombs) and non-lethal weapons (lasers, microwaves, electron beam generators). Physical destruction is executed as a planning technique among the integrated elements that work together to achieve information superiority.

3-53. Through CI collection, operations, investigations, debriefings or analysis, CI may identify threat collection assets (humans or systems) that are legitimate tactical targets and recommend neutralization by appropriate sea, land, or air forces.

COUNTERINTELLIGENCE SUPPORT TO INFORMATION ASSURANCE

3-54. Information assurance comprises information tasks that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

3-55. CI concentrates on the identification of foreign intelligence threats to information systems so system administrators have the information they need to emplace the proper measures to ensure their availability, data confidentiality, and the assurance that data has not been altered. In support of information assurance, CI may provide information on and countermeasures for the following:

- Hostile capabilities and intentions including which countries or their surrogates have the capabilities and the intent to target Army telecommunications and automated information systems.
- Army vulnerabilities including the degree to which telecommunications and automated systems are vulnerable.
- Awareness of techniques including the latest targeting techniques employed by adversaries.
- Unauthorized access including deliberate attempted penetration of Army automated data systems.

3-56. Army cyber CI elements assist Army computer network operations (CNO) with identification of adversaries who attempt to gain unauthorized access to Army networks and systems. CI can assist elements within the Army with information assurance by ensuring information holders know the adversary methods, techniques, and targets regarding our information and information systems.

COUNTERINTELLIGENCE SUPPORT TO CIVIL-MILITARY OPERATIONS

3-57. Civil-military operations (CMO) are activities of a commander that establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area to facilitate military operations, to consolidate and achieve operational U.S. objectives. CMO are conducted with, by, and through indigenous populations and institutions, U.S. Government agencies, international organizations, and other NGOs. CMO support the building of HN capacities to deter or defeat threats to internal stability. CI support to CMO consists of detecting, exploiting, deterring, or neutralizing adversarial intelligence collection targeting of CMO plans, operations, personnel, and equipment. The successful execution of CMO requires current intelligence and CI estimates which serve to provide situational awareness regarding the threat, help protect the force, and enhance the successful execution of CMO.

3-58. In order to protect the neutral image foreign entities hold regarding CMO, CI conducts limited to no operations in coordination to support CMO. With the exception of providing CI threat assessments regarding the locations in which CMO operations occur, CI attempts to dissociate its mission from the CMO community. This ensures that foreigners will not mistakenly assume that CMO personnel are operating under the intent and focus that CI personnel operate.

3-59. CI assets may conduct CI screenings of contract linguists or initiate the process of vetting local nationals assigned to conduct CMO with U.S. forces. The Civil-Military Operations Center (CMOC) serves as the primary interface between the U.S. armed forces, indigenous population and institutions, humanitarian organizations, intergovernmental organizations (IGOs) and NGOs, UN and other international agencies, multinational military forces, and other agencies of the U.S. Government. CI assets may coordinate with the CMOC to coordinate, deconflict, and execute debriefing operations with local

nationals, refugees, or displaced persons identified through the execution of CMO with reportable information of use to Army CI.

COUNTERINTELLIGENCE SUPPORT TO PUBLIC AFFAIRS

3-60. PA is the public information, command information, and community relations activities directed toward both the external and internal publics with interest in DOD. PA makes available timely and accurate credible information so that the public, Congress, and the news media may assess and understand the facts about national security and defense strategy. Effective PA enhances confidence in the force and its operations.

3-61. CI support to PA consists of detecting, exploiting, deterring, or neutralizing adversarial targeting of PA plans, operations, personnel, and equipment. The successful execution of PA operations requires current intelligence and CI estimates which serve to provide situational awareness regarding the threat, protect the force, and enhance the execution of PA operations.

3-62. In order to protect the neutral image foreign entities hold regarding PA operations, CI conducts limited to no operations that may impact PAO. With the exception of providing threat assessments regarding the CI threat in locations in which PAO will operate, CI attempts to dissociate its mission from the PAO community. This ensures foreigners will not mistakenly assume that PAO personnel are operating under the intent and focus that CI personnel operate.

3-63. CI assets will coordinate and integrate the support activity of vetting local nationals and contract linguists involved with PA operations with U.S. forces.

COUNTERINTELLIGENCE SUPPORT TO COMPUTER NETWORK OPERATIONS

3-64. CNO comprise computer network defense (CND), computer network attack (CNA), and related computer network exploitation (CNE) enabling operations. CND is conducted at all levels and consists of defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. CNA is operations conducted at the echelon above corps level to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CNE is done at the echelon above corps level and consists of enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.

3-65. CI elements tasked with support to CNO must be fully engaged in liaison with U.S. communications units, computer centers, and computer emergency response teams, as well as U.S. and HN intelligence, security, and law enforcement communities. Any abnormalities within the cyber world will be initially detected by these types of personnel who continuously work with systems and networks, and CI must have access to the information they possess. When possible, liaison with supported units' system administrators, help desks, network analysts, facility security managers, maintenance, technology protection personnel, and/or information system security officers (ISSOs) should occur to generate additional reporting of initial abnormalities with the physical aspect or within Army systems and networks.

3-66. Once abnormalities have been discovered on Army information systems and/or networks, cyber CI can begin to assist with the identification, exploitation, and neutralization of adversarial threats to U.S. information systems, networks, and interests via the Global Information Grid. CI can assist CNO personnel in detecting and identifying insider threats, destruction of systems, denial of service, compromise of database information, creation of malicious code, and determination of origin of intrusions. CI elements have the capability to examine the physical and virtual aspects of network architecture, applications, and software, Internet protocol (IP) addresses, users, locations, hardware and peripherals, and artificial constructs that pose a threat to Army CNO. Some of the specifics of how CI supports CNO are—

- Based on intrusion incident notification, provide investigative and analytical efforts to identify the intruders including the IP addresses, net users, locations, hardware and peripherals, and artificial constructs.

- Examine different applications, software, methodologies and TTP used by an adversary.
- Assist with identifying and detecting automation threat capabilities and identify U.S. vulnerabilities and measures for automation software, hardware, and infrastructure protection.
- Subsequently establish and maintain an incident database as well as databases of tools, threats, and fixes associated with intrusions for future trend analysis and to assist operational planners with COAs and network defenders in formulating system and network defenses.
- Assist in the preparation of war plans, contingency plans, and orders by identifying friendly C2 vulnerabilities and enemy C2 attack capabilities, assessing potential enemy C2 attack COAs against friendly forces, conducting risk assessments, and building and executing a C2 protect plan.
- Provide expertise in seizing electronic evidence including—
  - Recognizing evidence regarding electronically transferred information.
  - Preparing for search and seizure of electronic devices.
  - Conducting search and seizure of electronic devices (computers, wireless, cordless and cellular telephones, answering machines, electronic pagers, Fax machines, smart cards and magnetic stripe cards, identification card printers, scanners, printer, copiers, compact disc duplicators and labelers, digital cameras, video, audio, electronic game devices, home electronic devices, global positioning systems (GPSs), personal data assistants (PDAs), handheld computers, blackberries, security systems, video computer devices, storage media, skimmers, parasites, and other criminal technology. While this list is extensive, it is not all- inclusive because of new technology being fielded every day.

3-67. Computer network intrusions and CI investigations involving computers, networks, and other sophisticated technology require CI skills that differ from skills needed in the traditional CI arena. Therefore, cyber CI activities will be conducted by specially trained, certified, and equipped cyber CI special agents assigned to theater cyber CI organizations. However, when unable to receive support from cyber CI personnel, any CI special agent should be able to conduct at least preliminary investigative activities and search and seizure of electronic evidence operations.

Chapter 4

Counterintelligence Collection Program

EO 12333 provides both a mandate and the authority for DOD components to conduct CI collection. CI collection is the systematic acquisition of information about the capabilities, intentions, and activities of foreign intelligence and security systems (FISS) and international terrorist organizations (ITO) entities who engage in espionage, terrorism, sabotage, assassination, subversion, and intelligence collection targeting Army equities. It may include the acquisition of information on any adversary which presents a danger to lives, property, or security of forces or represents an intelligence collection threat to technology, information systems, or infrastructure.

GENERAL

4-1. Many Army and MI leaders often misunderstand the difference between CI and HUMINT collection. While both disciplines utilize similar methodologies (talking to a human source) and TTP (tactics used to collect and exploit the information), the overriding difference between the two collection activities is the type of information targeted and the objective of the collection.

4-2. CI collection is primarily threat focused. CI collection activities focus on detecting and identifying the known or suspected FISS and ITO collection targeting U.S. forces either for information exploitation or for potential targeting. The objective of CI collection is to be able to—

- Affect the FISS and ITO knowledge of the plans, intentions, and capabilities of U.S. forces.
- Deny FISS and ITO the information to target U.S. forces.
- Negate, mitigate, or disrupt the FISS and ITO collection capability.

HUMAN INTELLIGENCE AFFECTS FRIENDLY FORCE'S KNOWLEDGE OF THE ADVERSARY

4-3. HUMINT collection is requirements focused. HUMINT collection activities focus on identifying the plans, intentions, and capabilities of the adversary to support the commander's military decisionmaking process (MDMP). The objective of HUMINT collection is to affect U.S. force's knowledge of the adversary.

COUNTERINTELLIGENCE AFFECTS THE ADVERSARY'S KNOWLEDGE OF FRIENDLY FORCES

4-4. The CI collection program is conducted to gather the information the commander needs to make decisions to support the overall mission and help the commander shape the operational environment. The commander focuses the CI effort by carefully assigning missions and clearly defining the desired results. While using CI collection as a means of targeting, the use of single-source reporting could lead to targeting based on tribal, regional, or cultural differences rather than threat-based targeting. In all instances, CI reporting should be corroborated by other sources of information and/or intelligence disciplines to determine accuracy and truthfulness before targeting by the commander.

4-5. Special agents conduct CI collection activities to support the overall mission. These operations use techniques identified in AR 381-20. AR 381-10 contains 17 chapters that set forth policies and procedures governing the conduct of intelligence activities by DA personnel.

COUNTERINTELLIGENCE COLLECTION PROGRAM

4-6. The Counterintelligence Collection Program (CICP) encompasses three separate collection categories. Each category is distinct in the sensitivity and type of information being targeted, the source of the information, and the approval process required in the execution of the collection activity. The three categories of collection are offensive counterintelligence operations (OFCO), defensive source operations (DSO), and counterintelligence force protection source operations (CFSO).

- OFSO activities support Army, theater, ASCCs, and local intelligence requirements, as well as DOD, Joint Chiefs of Staff, combatant command, JTF, and multinational and national intelligence community strategic requirements to deter, detect, and neutralize espionage.
- DSO activities are only employed by units with a CI investigative and operational mission. DSO will not be employed in combat theaters, but should be proposed through the submission of a counterintelligence special operations concept (CISOC) and approved by the commander, INSCOM, or the single designee.
- CFSO uses source operations to collect protection, FISS and ITO collection, and threat I&W. Except for unit training, CFSO is conducted OCONUS to satisfy the supported commander's information requirements. CFSO is employed on the basis of a CFSO operations plan (OPLAN) approved by the supported commander or the C/J/G/S-2X if approval authority has been delegated by the ASCC or JTF commander.

4-7. Within each CICP category, there are three levels of operational activity. Each level represents the amount of control a CI special agent has over the operation and its sensitivity. The three levels are casual, developmental, and controlled:

- **Casual.** One-time sources or casual contacts that can provide atmospheric data, protection, and threat I&W. The CI special agent has minimal control over the operation beyond planning and coordination of meetings and debriefing the source regarding knowledge on areas of interest to the CI special agent. Casual sources—
  - Include all CI sources established during elicitation, CI screenings, CI debriefings, and overt liaison with military and government officials.
  - Are never tasked to gather or obtain information on behalf of U.S. forces; however, those U.S. forces personnel whose travel and official duties require them to be debriefed may be pre-briefed before their travel or activity to understand the information requirements of the CI special agent.
  - Will be locally coded by the CICA/2X for future reference, to establish a reporting history and to avoid redundant contacts with multiple intelligence elements. Liaison contacts will never be considered for developmental and controlled operational activities.
- **Developmental.** Sources which have been routinely contacted and can provide more detailed information than a casual source. Developmental sources—
  - Include any contacts within OFCO, DSO, or CFSO who require further assessment to validate their potential as a controlled source.
  - Have demonstrated positive views or sentiment towards U.S. forces.
  - Are never tasked to gather or obtain information on behalf of U.S. forces. Operational interest must be obtained before transitioning a casual source to a developmental source. Operational interest is granted after submission of basic source data (BSD) reports and request for operational interest to the responsible 2X. Records checks are done with all applicable agencies in the AOR; deconfliction has been conducted by the 2X/CICA; and permission is granted by the responsible 2X.

- Will be locally coded by the CICA/2X for future reference, to establish a reporting history and to avoid redundant contacts with multiple intelligence elements.

- **Controlled.** Sources who have an established reporting history, are deemed credible, and who have been vetted by CI elements. Controlled sources have also agreed to meet and cooperate with the CI special agent for the purpose of providing information. Controlled sources—
  - Can be tasked to provide the CI special agent with specific information based upon their employment, social, or geographic associations. Meetings between the CI special agent and the controlled source will be limited to the CI special agent, the operational management element, CICA/2X and commander unless otherwise directed by the commander and 2X. A lead development report (LDR) must be submitted to and approved by the responsible CICA/2X before transitioning a developmental source to a controlled source.
  - May also be referred to as an asset.

COUNTERINTELLIGENCE DEBRIEFINGS, SCREENING, AND LIAISON

4-8. A majority of the information obtained by CI special agents comes during the course of overt collection missions. These missions include debriefings, screenings, and liaison.

COUNTERINTELLIGENCE DEBRIEFINGS

4-9. CI debriefings focus on two different types of targets. Debriefing of repatriated U.S. personnel or SCAs and personnel who are pre-briefed and debriefed as part of an approved CI operation or project. CI personnel assigned to combat units may also participate in intelligence debriefing of U.S. or coalition patrols or other tactical elements that may support CCIRs. Debriefings are conducted for two reasons:

- As a collection activity that supports CI or other collection reporting requirements with the information being submitted via an IIR.
- Identify potential incidents of CI interest that may be within Army CI investigative authority.

Debriefing of Special Category Absentees

4-10. These debriefings are generally conducted on persons whose intentions and existing evidence, at the time of the offense, do not support their involvement in the commission of a national security crime or incident of CI interest. However, due to the nature of their absence and circumstances concerning their contact with potential FISS and ITO, they should be debriefed to identify incidents of CI interest. Debriefings of SCA personnel returned to U.S. control will, at a minimum, focus on the following:

- Circumstances surrounding their absence, including motivation and planned destination.
- Persons or organization the SCA came into contact with or provided assistance to the SCA.
- Visits to any foreign diplomatic or government organizations during the absence.
- Travel to or through a country during the absence and all activities that occurred during the travel.
- Contact with a representative or agent of a foreign government or terrorist organization.
- What type of information, either classified or unclassified, the SCA provided to any unauthorized person.

Debriefing of Defectors

4-11. Debriefing of U.S. defectors under the authority of Army CI will be conducted upon their return to U.S. control. Debriefings of defectors will be conducted regardless of whether or not they had access to classified information. Debriefings of defectors will, at a minimum, focus on the following:

- Circumstances and motivation surrounding the defection and their planned destination.
- Persons or organization with whom the defector came into contact or provided assistance to the defector.
- Full descriptions and identifying data of foreign intelligence officers, interrogators, or other officials with whom the defector had contact.
- Source of funding during the defectors absence.
- Whether or not defectors used aliases, false identifications, or concealed their identities. If so, how and from whom was the documentation obtained?
- Identification and disposition of any computer, media, hardware, military equipment and/or technology or any classified or unclassified documents the defector had possession of or gave to any unauthorized person.
- Travel details including mode of transportation, itinerary, countries traveled to or through, and means and documentation required to cross international borders.
- Details of all interrogations or interviews the defector underwent: details of conversations, identity and physical descriptions of interrogators, interrogation methods, defector's cooperation, interrogator responses to defector's refusal to answer, cooperate, or inability to answer a question.
- Any attempts to obtain the defector's assistance in providing information on any U.S. person or organization, offers to employ the defector in intelligence collection or other activities, and any arrangements to reestablish contact at a later time.
- Nature and extent of any publicity or media exposure given to the defector.
- Foreign government's response to the defector's presence in another country.
- Complete details of any contacts with any other U.S. defectors to include identifying data, names, physical descriptions, units of assignment, clearance and access to classified information, family background, places of residence in the United States, last known location, known or suspected cooperation with foreign intelligence or other officials, reasons for defection, current attitude concerning their defection.

Debriefing of Repatriated U.S. Prisoners of War or Detainees

4-12. When directed by a higher authority, CI special agents may conduct intelligence debriefings of Army military, civilian, and contract personnel who have been detained, captured, or imprisoned by foreign military forces, foreign governments, terrorist groups, or intelligence services. These debriefings will, at a minimum, focus on the following:

- Circumstances of capture or detention.
- Physical descriptions and full identifying data of foreign military, intelligence, law enforcement and government officials, terrorists, key leaders.
- Locations of command control facilities, military installations, safe houses, detention facilities and weapons storage sites.
- Description of interrogation techniques, questions asked, and information provided.

- If the POW/detainee was directed or asked to perform any activity after release and detainee's response.
- Identity and location of the POW/detainees or defectors, their treatment, and physical and mental condition.
- Description of any sensitive or classified information, materiel, or equipment captured or compromised.

Debriefing in Support of a Counterintelligence Project or Operation

4-13. These types of debriefings are generally conducted by operational or theater and strategic CI elements which maintain a CAP with supported units, CI units who participate in the Tactical Intelligence and Related Activities Program, or other CI projects or operations approved for specific purposes to generate CI reporting and lead generation.

4-14. The target of these types of debriefings are Army personnel who conduct official or approved unofficial travel to areas of intelligence interest or whose official business brings them into contact with foreign officials or persons. During these types of projects or operations, the CI asset is pre-briefed on information of CI interest and is given strict instructions on their conduct during the travels or meetings. The CI asset is then debriefed upon their return to obtain any information of CI or general intelligence interest.

COUNTERINTELLIGENCE SCREENING

4-15. CI screening is a systematic process for obtaining information of CI interest from a specific person or target audience. Information of CI interest includes all SCICRs established in AR 381-20, CCIRs, or any information that includes, but is not limited to, the plans, intentions, capabilities, methods of operation, personalities, structure, and personal associations with any FISS and ITO entity. CI screening uses a variety of questioning techniques to obtain information. This includes—

- Interviewing methods using basic interrogatives to identify and exploit information of CI interest.
- A structured debriefing format utilizing a prepared question list when the source has knowledge of a specific topical interest.
- Elicitation utilizing a discreet form of questioning which does not let the source know the specific area of interest of the CI special agent.

4-16. Each of these methods can be used or combined dependent upon the situation. For example, in an LEP screening process, the CI special agent can prepare specific questions that the source may have knowledge of. During the screening interview, if the source provides a lead outside the scope of the debriefing questioning list but of CI interest, the CI special agent can transition to an interview format to gain all the additional information the source may have on the subject. If the CI special agent believes the source may have knowledge of other types of information, the CI special agent can probe for other knowledgeable areas using elicitation techniques.

Note. CI screening normally is non-confrontational unless the source initiates a hostile environment and forces the CI special agent to maintain control through the exercise of the CI special agent's official authority. CI screening should **not** be characterized or executed using any of the interrogation approaches defined in FM 2-22.3.

4-17. CI elements should designate CI screening as high priority collection activity which can produce significant intelligence reporting, identify persons as potential controlled sources, cue other intelligence assets, and generate leads for potential investigative activities. CI screening is the primary tool used to vet LEPs for suitability and potential risks to U.S. personnel while employed by U.S. forces. It is also used by CI personnel to canvass local population centers, traffic control points (TCPs), and refugee or displaced

persons migration for information of CI interest. CI screening can also be used to identify potential sources for the CFSO and DSO programs.

4-18. During the CI screening program the sources may be screened to determine their potential to answer collection requirements or to identify individuals who match a predetermined source profile. Personnel who cannot specifically answer CI requirements but may be able to answer other collection requirements can be identified and the lead passed to a HUMINT collection team (HCT) via a Notice of Intelligence Potential or other localized procedures identified in unit SOPs.

4-19. Successful CI screening requires dedicated resources and support from the chain of command. Pre-operational planning should include dedicating specific CI assets to be the focal point for coordinating and conducting all CI screening. All necessary equipment, facilities, and support personnel should also be identified in OPLANs and coordinated for in advance of executing the CI screening program. For example:

- Equipment includes biometric systems used to identify and track LEPs, third-country nationals or original screened individuals after the screening. This allows CI special agents and/or intelligence analysts to potentially identify persons associated with events or intelligence reporting if they have been previously screened.
- Facilities include dedicated space that offers privacy and security during the screening process. CI screenings should not afford those personnel waiting to be screened the opportunity to hear previous screenings. Lack of privacy allows a potential infiltrator or FISS and ITO agent the opportunity to hear ongoing screening interviews and formulate plausible answers and information to evade further scrutiny by CI elements. Pre-screening security checks of all sources should be conducted to identify potential weapons. In hostile or non-secure environments, coordination for security forces should be conducted to ensure the safety of U.S. forces, and the screening audience.
- Interpreters should be identified in the pre-operational planning process. This should include what language and dialects will be required and the number of interpreters based upon mission requirements. Additionally, any specific security clearance requirements should be included in the request and planning documents.
- Coordination should be included in all OPLANs to delineate responsibilities, identify supporting organizations and gain command approval. OPLANs should include the CI screening mission in the conduct of patrols, cordon and search and TCPs. This provides the CI element the leverage to conduct the mission when local units are apprehensive about CI personnel operating outside the installation or base camp.
  - LEP screening should include coordination with the unit protection officer, supporting MP units, installation security elements, and contracting office. CI Screening of LEPs is not an employment activity, but rather a decision point to assist the contracting office and the commander to adjudicate the suitability of a host nation, TCN or other indigenous person to work for U.S. forces.
  - If the CI element identifies that the person may be a protection risk based on the person's background, activities, or associations of known FISS and ITO entities, the person should be identified as a protection risk. It is commanders' responsibility to determine if they are willing to accept that risk.

Counterintelligence Support to Joint Interrogation and Debriefing Centers

4-20. During combat and other contingency operations, CI normally will be included in the staffing and support requirements for JIDC operations. While the priority for intelligence collection during JIDC operations is focused on CCIRs and other HUMINT-specific collection requirements, JDIC operations offer an excellent opportunity for CI collection. Enemy prisoners of war (EPWs) and detainees held in JDIC facilities will include FISS and ITO personnel who can answer specific CI requirements including,

but not limited to, the plans, intentions, capabilities, methods of operation, personalities, structure, and personal associations of FISS and ITO elements targeting U.S. forces.

4-21. CI Special agents supporting JIDC operations will normally sensitize or provide detailed CI requirements to the JDIC operations element. All interrogation personnel will use these requirements to identify personnel who have information of CI interest. When an EPW or detainee is identified as having information of CI interest, the CI special agent will screen the identified person separately from HUMINT screening and interrogation activities. While there is no prohibition of CI special agents being present during interrogations conducted by trained and certified interrogators, generally the limited numbers of CI resources do not permit this approach.

Locally Employed Person Screening

4-22. LEP screening is conducted primarily to identify individuals who may be a security risk. It can, however, be used as a means to obtain intelligence information or to identify personnel with placement and access to be used for source operations. LEP screening should be conducted as a precondition to employment and repeated periodically throughout the course of employment. It should also be conducted whenever a local employee is promoted or placed in a new job position.

4-23. CI Special agents should coordinate with security and hiring authorities to have CI screenings conducted as part of the normal hiring process before granting unescorted access to the installation. LEP screening must be conducted in a secure environment and out of the hearing and sight of other employees. While conducting the screening the CI special agent should pay special attention to any indicators of deception. During the screening process, the use of an interpreter is paramount to maintain accuracy in recording the information obtained from the LEP. Formal written reports of the screening must be maintained.

4-24. During LEP screenings, several factors must be determined before acceptance for employment. Following the screening, the CI special agent must assess—

- The suitability of the person in relation to the job to be performed. Is the individual attempting to access an area above the individual's level of knowledge, skills, and experiences?
- Whether the individual has any suspected FISS and ITO associations?
- What family associations the person has that could lead to possible hostage situations?
- If the person has outside placement and access that could be exploited for potential use as a CI source?
- If the individual has any special skills or languages that may be leveraged to support ongoing collection missions?

Note. If a person has potential FISS and ITO connections, it does not automatically mean this person cannot be used as a CI source or exploited by CI units or OGAs. If a person is willing to cooperate with these units or agencies or is susceptible to control and direction, then commanders should give consideration to these activities. Persons with potential FISS and ITO connections could provide information pertinent to ongoing investigations and operations such as the location of any hostages, personnel behind recent or future attacks, locations of safe houses or houses used to construct improvised explosive devices (IEDs).

4-25. If an LEP is reported or found through background checks to have derogatory information, a CI screening should be conducted immediately. The CI special agent should attempt to determine the severity of the derogatory information and to what extent this information may be exploited. These derogatory initiated screenings should be recorded electronically and maintained for the protection of the agent. The information derived because of this screening should be reported to the command and the command of adjacent units or camps and maintained in local records to preclude the future rehiring of the individual.

COUNTERINTELLIGENCE LIAISON

4-26. CI special agents conduct liaison to obtain information, gain assistance, and coordinate or procure material. The nature of CI activities and the many legal restrictions imposed, including SOFAs or other agreements, make the collection of intelligence information during peacetime largely dependent on effective liaison.

4-27. CI special agents use liaison to obtain information and assistance and to exchange views necessary to understand our liaison counterparts. During transition from increased tension to open hostilities, the liaison emphasis shifts to support the combat commander.

4-28. CI special agents must establish liaison with appropriate agencies before the outbreak of hostilities. Information and cooperation gained during this period can have a major impact on the effectiveness of both intelligence and combat operations. The use of interpreters occurs often in liaison, as foreign language proficiency is not a requirement for the CI special agent.

4-29. Liaison with appropriate U.S., HN, and allied military and civilian agencies is fundamental to the success of CI operations and intelligence support to commanders. In many cases, full-time liaison officers (LNOs) or sections are necessary to maintain regular contact with appropriate organizations and individuals. In addition to national agencies, numerous local agencies and organizations also provide assistance and information.

4-30. A basic tenet of liaison is *quid pro quo* (something for something) exchange. While the CI special agent sometimes encounters individuals who cooperate due to a sense of duty or for unknown reasons of their own, an exchange of information, services, material, or other assistance normally is part of the interaction. The nature of this exchange varies widely, depending on location, culture, and personalities involved. The spectrum of liaison tasks ranges from establishing rapport with local record custodians to coordinating sensitive multinational operations at the national level of allied nations. Commanders with CI assets involved in liaison should provide the following:

- Liaison objectives, which are types of information to be collected, methods of operations unique to the area, and command objectives to be accomplished.
- Source coding procedures.
- Report numbering system.
- Procedures for requesting sanitized trading material information.
- Authority under which the specific liaison program is conducted and guidelines for joint and multinational operations.
- SOPs that cover related aspects, such as funding, IIR procedures, source administration, and AORs and jurisdiction.

4-31. Operational benefits derived from CI liaison include—

- Establishing working relationships with various commands, agencies, or governments.
- Arranging for and coordinating joint and multinational multilateral investigations and operations.
- Exchanging operational information and intelligence within policy guidelines.
- Facilitating access to records and personnel of other agencies not otherwise available. This includes criminal and subversive files controlled by agencies other than MI. Additionally, access includes gaining information via other agencies when cultural or ethnic constraints preclude effective use of U.S. personnel.
- Acquiring information to satisfy U.S. intelligence collection requirements.

- Limitations on liaison activities. These limitations include—
  - Prohibitions against collection of specific types of information or against contacting certain types of individuals or organizations.
  - Memorandums of understanding with other echelons delineating liaison responsibilities.
  - Delineation of areas of responsibility of subordinate elements.
  - Director of Central Intelligence Directives (DCID).
- Type, method, and channels of reporting information obtained from liaison activities.
- Use of ICF.

4-32. OCONUS, CI liaison provides support to a number of diverse U.S. Government agencies. This support ranges from conducting tactical operations to fulfilling national level requirements generated by non-DOD federal agencies. Individuals contacted may include private individuals who can provide assistance, information, and introductions to the heads of national level host country intelligence and security agencies.

4-33. In CONUS, CI liaison provides assistance in operations and investigations, precludes duplication of effort, and frequently provides access to information not available through other CI channels. Agents should maintain a POC roster or list of agencies regularly contacted. Agencies normally contacted on a local basis include—

- Military G-2, S-2, and personnel sections of units in the area.
- G-9 and S-9 representatives.
- MP and PMO.
- Army CIDC for information relating to incidents that overlap jurisdictions.
- Civilian agencies such as state, county, or local police departments; state crime commissions; state attorney general offices; and local courts.
- Local offices of Federal agencies such as the FBI, Immigration and Naturalization Service, Border Patrol, Drug Enforcement Agency, and similar security agencies.
- Appropriate DOD activities such as Naval Criminal Investigation Service and Office of Special Investigations (OSI) of the U.S. Air Force.

4-34. The DA G-2 is responsible for liaison with the national headquarters of the intelligence community and other agencies for policy matters and commitments. CG, INSCOM, is the coordinating authority for liaison with the FBI and other Federal agencies for coordinating operational and investigative matters.

4-35. Many countries exercise a greater degree of internal security and maintain greater control over their civilian population. For this reason, the national level intelligence and security agencies frequently extend further into the local community in other countries than they do in the United States. Security agencies may be distinctly separate from other intelligence organizations, and police may have intelligence and CI missions in addition to law enforcement duties. In some countries, the police, and usually another civilian agency, perform the equivalent mission of the FBI in the U.S. This other civilian agency frequently has a foreign intelligence mission in addition to domestic duties. CI special agents must be familiar with the mission, organization, chain of command, and capabilities of all applicable organizations they encounter.

4-36. Adapting to local culture is sometimes a problem encountered by the CI special agent involved in liaison. Each culture has its own peculiar customs and courtesies. While they may seem insignificant to U.S. personnel, these customs and courtesies are important to local nationals. Understanding a country's culture and adhering to its etiquette are very important. What is socially acceptable behavior in the United States could very well be offensive in other cultures. Knowing the local culture helps the CI special agent understand the behavior and mentality of a liaison source. It also helps in gaining rapport and avoiding embarrassment for both the liaison source and the CI special agent. In many cultures, embarrassing a guest

causes "loss of face." This inevitably undermines rapport and may cause irreparable harm to the liaison effort.

4-37. The CI special agent also must understand the capabilities of agencies other than our own. Knowledge of the liaison source's capabilities in terms of mission, human resources, equipment, and training is essential before requesting information or services. Information exchanged during the conduct of liaison is frequently sanitized. Information concerning sources, job specialty, and other sensitive material relating to the originator's operations may be deleted. This practice is common to every intelligence organization worldwide and should be taken into account when analyzing information provided by another agency.

4-38. The CI special agent may have to deal with individuals who have had no previous contact with U.S. agencies and who are unsure of how to deal with a U.S. intelligence agent. CI special agents must remember that to the liaison source, they represent the people, culture, and government of the United States. The liaison source assumes the behavior of the CI special agent to be typical of all Americans.

4-39. The CI special agent may have to adapt to unfamiliar food, drink, etiquette, social custom, and protocol. While some societies make adjustments for an "ignorant foreigner," many expect an official visitor to know local customs. The CI special agent must make an effort to avoid culture shock when confronted by situations completely alien to the agent's background. The CI special agent also must be able to adjust to a wide variety of personalities.

4-40. In some countries, government corruption is a way of life. The CI special agent must be familiar with these customs if indications of bribery, extortion, petty theft of government goods and funds, or similar incidents are discovered in the course of liaison. When corruption is discovered, request command guidance before continuing liaison with the particular individual or organization. Regardless of the circumstances, exercise caution and professionalism when encountering corruption.

4-41. The CI special agent must know any known or hidden agendas of individuals or organizations. Occasionally, due to the close professional relationship developed during liaison, a source may wish to present a personal gift. If possible, the CI special agent should diplomatically refuse the gift. If that is not possible, because of rapport, accept the gift. Any gifts received must be reported in accordance with AR 1-100. The gift can be kept only if a request is submitted and receives approval.

4-42. Records and reports are essential to maintain continuity of liaison operations and must contain information on agencies contacted. It is preferable to have a file on each organization or individual contacted to provide a quick reference concerning location, organization, mission, and similar liaison-related information. Limit information to name, position, organization, and contact procedures when the liaison contact is a U.S. person. The CI special agent should obtain consent from the U.S. liaison contact to maintain general re-contact data for future reference. For liaison contacts with foreign persons, formal source administrative, operational, and information reporting procedures are used.

CONTROL OF SOURCE INFORMATION

4-43. All collection operations require keeping records on CI military sources. This holds true for liaison contacts as well as casual or recruited sources. Data on CI military sources will be entered into appropriate echelon source registries and, in the future, the planned Integrated Defense Source Registry (IDSR). This type of information, including biographic, motivational, and communications procedures, are maintained in CI channels.

4-44. Control of source information will not preclude passage of this type of information from one echelon to another for necessary approvals. In handling source information, strictly adhere to the "need-to-know" policy. The number of persons knowing about source information must be kept to a minimum. (See AR 381-20 for more information on the control of source information and CI collection and reporting activities.)

UNIT COUNTERINTELLIGENCE REQUIREMENTS MANAGEMENT

4-45. Unit requirements managers will—

- Develop ISR synchronization requirements plans to satisfy the CI collection requirements of the supported commander.
- Plan and oversee the CI collection operations designed to support current and future military operations.
- Ensure that CI collection requirements are effectively communicated to those conducting collection or source operations.
- Track, monitor, and evaluate the effectiveness of the collection mission and provide statistical data on collection sources, activities, and reporting as required.

4-46. Collection planning is an important part of the management of CI collection operations because it determines how a collection requirement will be satisfied. Collection planning is essential to maximizing resources, ensuring responsiveness, properly focusing collectors, and minimizing risk.

4-47. The Army CI requirements manager will ensure that collection elements with the appropriate capability, resources, and location are tasked to satisfy levied requirements. Providing input to the ISR synchronization requirements plan requires knowledge of FISS and ITO, the availability of resources for collection, collection priorities, and geographic areas where the collection activity will be accomplished.

4-48. ISR plans should be modified as frequently as dictated by world events, military operations, new requirements, and modifications to existing requirements due to intelligence gaps. CI collection to support ASCC or joint operations normally will be documented in the CI appendix to an OPLAN and will be executed under an OPORD. The typical CI collection plan may be organized including the following elements:

- **Mission.** Identity of CI collection requirements to support a mission, operation, geographic area, or command.
- **Concept of operation.** Identity of collection element; C2 structure; collection focus.
- **Coordination.** ATCICA, 2X, chief of station, chief of mission, and OGAs.
- **Operational considerations.** Source restrictions, OPSEC measures.
- **Administrative support requirements.** Reporting system, communications architecture, operational reporting requirements.
- **Operational expenses.** Projected ICF expenditures, expense codes, incentives, appointment of alternate custodians, accountability procedures.

4-49. ISR plans should assess the capabilities of the CI collection element by addressing the following issues:

- **Capability.** The capability of the collection element to satisfy the requirement and the existence of a source which can answer the requirement.
- **Access.** Whether the collection element has the ability to access the source.
- **Resources.** The resources available to the collection element to accomplish the required collection and the identity of any additional resources.
- **Source development potential.** The capability of the collection element to develop a source where none exists.
- **Priorities.** The relative priority of new requirements compared to those already levied.

STANDING COUNTERINTELLIGENCE COLLECTION REQUIREMENTS

4-50. SCICRs serve as the basis for CI collection planning and implementation. SCICRs are promulgated by DIA J-2 CI based on general collection themes identified by the intelligence community and coordinated with CI analysts throughout DOD. All Army CI elements, within the limits of their mission, assigned priorities, resources, location, and collection capability, have an obligation to collect and report the following categories of information:

- Foreign intelligence activities.
- Technology transfer.
- WMD.
- Transnational terrorist groups.
- Cyber espionage.

COUNTERINTELLIGENCE SUPPORT TO THREAT AND VULNERABILITY ASSESSMENTS

4-51. TAs and VAs are studies conducted by CI personnel to provide a supported command or agency a picture of the FISS and ITO threat or the unit or agency's susceptibility to FISS and ITO intelligence collection. TAs are focused on known or suspected FISS and ITO collection capabilities in a specific geographic area and can be used for educational and security planning purposes. TAs are standalone documents. VAs are conducted on a specific target (for example, command, agency, installation, subordinate element, headquarters, operation, facility, or program) and are tailored to the needs of each requestor. The objective of the VA is to provide a supported command or agency a realistic tool with which to evaluate internal protection or security programs, and to provide a decisionmaking aid for the enhancement of these programs. VAs must include a TA.

4-52. TAs include—

- General political, social, and economic demographics for the target area that may be exploited by a FISS and ITO element to conduct operations.
- Known or suspected associations between FISS and ITO elements and governmental agencies or personnel who may indicate support, direction, or funding of FISS and ITO elements.
- Governmental and civilian populace attitudes (positive or negative) towards U.S. policies or culture.
- Specifics on known or suspected FISS and ITO elements including—
  - Identities of known members.
  - Identities of leadership members.
  - Capabilities, plans and intentions.
  - Methods of operation.
  - Previous acts, situations, or events for which the FISS and ITO has been responsible, has taken credit, or has been associated.

4-53. VAs include—

- Evaluating adversarial intelligence multidiscipline intelligence collection capabilities, collection and other activities, and CCIRs.
- Identifying friendly activity patterns (physical and electronic), friendly physical and electronic signatures, and resulting profiles.
- Monitoring or collecting communication and electronics (C&E) transmissions to aid in VAs, and providing a more realistic and stable basis from which to recommend countermeasures.
- Identifying vulnerabilities based upon analysis of collected information and recommendations of countermeasures.
- Analyzing the effectiveness of implemented countermeasures.

This page intentionally left blank.

Chapter 5

Analysis, Tools, and Production

Intelligence analysis is the cognitive process of receiving and interpreting information from every available asset, and integrating that information into the overall view of the operational environment. Analysis requires organization of information into categories and identifiable patterns (relationships among the categories), based on the information collection requirements. Intelligence analysis is the art of knowing and understanding the enemy's doctrine, culture, weapon capabilities, TTP, religion, beliefs, and idiosyncrasies. In addition, an intelligence analyst is fully aware and knowledgeable of the limitations and capabilities of U.S. forces.

GENERAL

5-1. In order for commanders to effectively complete the operations process, they must have information and intelligence. The intelligence process satisfies this need by providing the commander with intelligence regarding the threat, operational environment, and the situation. Four steps constitute the intelligence process: plan, prepare, collect, and produce. Additionally, there are four activities that occur across the four steps of the intelligence process: generate intelligence knowledge, analyze, assess, and disseminate. The four continuing activities plus the commander's input drive, shape, and develop the process. They can occur at any time during the process. The intelligence process steps and intelligence continuing activities are applied to CI to ensure synchronization with the all-source intelligence mission and collection. (See figure 5-1.)

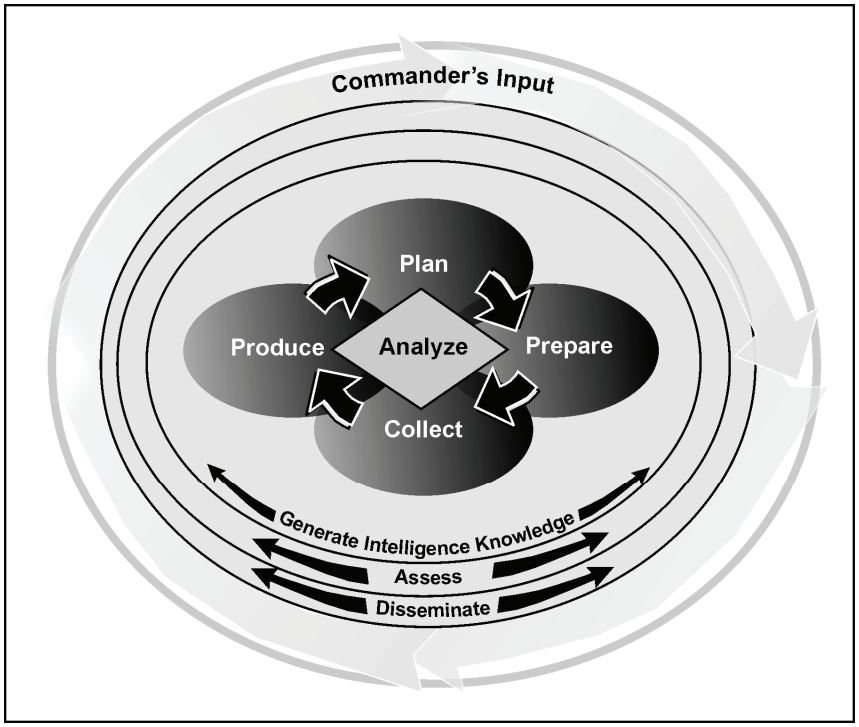

Figure 5-1. Intelligence process

5-2. Intelligence analysis also involves separating useful information from extraneous information, using experience and reasoning, and reaching a conclusion based on fact and/or sound judgment. The conclusion is based on the intelligence analyst's experience, skill, and knowledge of the various intelligence disciplines; ISR; an understanding of the operational environment; CCIRs; and an in-depth understanding of the adversary's behavior patterns. The intelligence analyst's knowledge must encompass many things; for example, the analyst—

- Interprets the intelligence reached throughout the intelligence analysis process.
- Realize that if not disseminated and exploited, the intelligence becomes useless.
- Knows friendly organizations, systems, doctrine, and tactics as well as those of coalition partners.

5-3. Analysis is not proprietary to the trained intelligence analyst. CI special agents, commanders, and leaders must conduct analysis to provide input into the intelligence process and to help drive the operations of all CI elements. CI analysis, tools, and production are essential elements in supporting CI activities; investigations, collection, and technical services and support. CI analysis of the FISS and ITO collection threat is critical to the establishment of protection measures by commanders at all levels.

5-4. Intelligence and threat analysis also provides focus for the implementation of CI support to the combatant command during military operations. CI analysis supports operational planning and provides direction to CI activities. CI analysis conducted in the 2X CI analytical cell concentrates on satisfying local PIRs, and on redirecting CI collection efforts. (See TC 2-33.4 for more information on intelligence analysis.)

5-5. The following are some areas that may be addressed in conducting CI analysis:

- Multidiscipline FISS and ITO operations.
- Activities and disinformation or deception operations.
- Illegal sale, transfer, or acquisition of DOD-controlled technologies, including WMDs.
- Terrorism, sabotage, unauthorized penetration or degradation of computer systems and related security threats.

5-6. CI analysis involves the actions taken to evaluate the information provided by all CI sources at a given echelon to determine interrelationships, trends, and contextual meaning. While called "single discipline," the analyst reviews and incorporates, as necessary, information from other disciplines and all-source analysis to provide a contextual basis for the CI analysis. Single-discipline CI analysis is conducted primarily by the analysis and control element (ACE). CICAs and CI OMTs also conduct analysis to a lesser degree, based on the information from CI sources at their echelon.

5-7. Analysis does more than simply restate facts; it puts information into context as it applies or affects the consumer. CI analysis uses the analytical principles of processing data inputs, factoring different variables, and developing a hypothesis that is the foundation for predictive analysis. This in turn is used during the MDMP, COA development, operational planning and the targeting process. The analyst formulates a hypothesis based on available data, assesses the situation, and explains what the data means in logical terms that the user can understand. There are two basic thought processes used mutually by analysts to study problems and reach conclusions: induction and deduction.

5-8. Induction is the process of formulating hypotheses on the basis of observation or other evidence. It can best be characterized as a process of discovery when the analyst is able to establish a relationship between events under observation or study. Induction, or plausible reasoning, normally precedes deduction and is the type of reasoning analysts are required to perform most frequently.

5-9. Deduction is the process of reasoning from general rules to particular cases. The analyst must draw out, or analyze, the premises to form a conclusion. Deductive reasoning is sometimes referred to as demonstrative reasoning because it is used to demonstrate the truth or validity of a conclusion based on certain premises.

5-10. CI analysis assists the G-2 in the identification and characterization of the human component of FISS and ITO intelligence collection operations and its effects on friendly and enemy operations. It carefully examines the various component groups and their predicted reaction to friendly force operations.

5-11. The CI analytical effort assists the overall all-source process by helping to identify specific actions and motivational factors that should strengthen the local population's support of the United States or at least weaken its support of the enemy and to provide information on the transient (refugees, displaced persons, third-country nationals) population and its effects on friendly and enemy operations. In addition to the above, analysts—

- Closely examine the current and potential threat to identify all factors, such as morale, motivation, training, and beliefs that would both positively and negatively affect adversary capabilities.
- Identify formal and informal leaders of hostile, neutral, and friendly groups and how their influence is likely to affect operations.
- Develop overlays, databases, and matrices, as required, to support intelligence preparation of the battlefield (IPB). These overlays may represent a wide variety of intelligence issues, including operational environment infrastructure (for example, electrical power grid), population density; ethnic, religious, or tribal affiliation; and no-strike or collateral damage.
- Provide their products to the C/J/G/S-2, the all-source analysts and CI analysts of the ACE, the HOC, the C/J/G/S-2X, and CI collection units as required.

ANOMALIES, SIGNATURES, AND PATTERNS

5-12. A critical component of CI analysis is the incorporation of different anomalies, signatures, or patterns that may be indicative of FISS and ITO targeting of U.S. forces.

- Anomalies are irregular or unusual activities that may cue the analyst on the existence of FISS and ITO activity. Anomalies may consist of repeated but subtle tests of systemic or security procedures (for example, an LEP who attempts to work in areas for which they are not cleared).
- Signatures are indicators of potential FISS and ITO methods of operations including static surveillance of U.S. forces installations, elicitation of LEPs or Service members.
- Patterns are repeated incidents that may be similar in nature or dissimilar events that occur in a specific location or time span that may indicate potential FISS and ITO targeting or information exploitation.

5-13. Analysis of anomalies, signatures, and patterns can allow analysis to help drive CI activities and develop pro-active operations to negate, mitigate, degrade, or exploit FISS and ITO collection activities.

COUNTERINTELLIGENCE THREAT ANALYSIS

5-14. CI analytical products provide information to support commanders, their staff, and unit. CI analysis is an integral part of CI collection. CI analysis occurs throughout the CI collection process but can be divided into four primary categories: analytical support to operational planning and targeting, operational analysis and assessment, source analysis, and single-discipline CI analysis and production.

5-15. The CI analyst uses the tools and skills identified in this chapter and in TC 2-33.4. The intelligence analyst focuses on "how we see the opposition" and "how the opposition sees us." The CI analyst must also focus on how to counter the opposition's collection efforts. Where the intelligence analyst is a subject matter expert on the opposition, the CI analyst, in addition to having an in-depth understanding and expertise on foreign intelligence collection capabilities, must have a good working knowledge of our own force. The CI analysis assets of the ACE must be fully integrated into the DCSG-A. They require access to

all-source data that is applicable to CI analytical products. The principles and techniques identified in TC 2-33.4 apply equally in CI analysis.

5-16. CI analysis and production is focused on FISS and ITO threat collection activities that include HUMINT, SIGINT, geospatial intelligence (GEOINT), and TECHINT. The focus of the CI analysis of each of these disciplines is not only on the threat entity or entities operating in the area but also on the intelligence products most likely being developed through their collection activities. While analysis is purely a cognitive process, the ability to organize and manipulate data to maximize the efficiency of the analytical process should be fully automated (data storage, sorting, and filing). The process of countering each of these disciplines involves—

- Threat assessment.
- Vulnerability assessment.
- Development of countermeasures options.
- Countermeasures implementation.
- Countermeasures evaluation.

COUNTER-HUMINT ANALYSIS

5-17. The CI analytical effort should attempt to identify the threat HUMINT cycle (collection, analysis, production, targeting) and threat personalities. To produce a complete product, the CI analyst may need access to considerable data and require significant resources. The CI analyst will require collection in the areas of subversion, espionage, sabotage, terrorism, and HUMINT supported activities.

5-18. Collection of friendly data is also required to substantiate analytical findings and recommendations. Consistent with time, mission, and availability of resources, efforts must be made to provide an analytical product that identifies threat collection efforts.

COUNTER-SIGINT ANALYSIS

5-19. The CI analyst requires SIGINT data collection to support VA and countermeasures evaluation. Validation of vulnerabilities (data collectable by threat SIGINT) and the effectiveness of implemented countermeasures (a before-and-after comparison of electromagnetic spectrum and data) will be nearly impossible without active and timely collection as a prerequisite to analysis. The CI analyst requires a comprehensive, relational database consisting of threat SIGINT systems, installations, methodology, and associated SIGINT cycle data.

5-20. In addition, all friendly C&E systems and user unit identification must be readily available, as well as a library of countermeasures and a history of those previously implemented countermeasures and results. Ideally, the CI analyst should, at any given time, be able to forecast threat SIGINT activity. However, such predictions must rely upon other CI, HUMINT, SIGINT, and GEOINT collection as well as access to adjacent friendly unit CI files. Information on threat SIGINT must be readily accessible from intelligence elements higher as well as lower in echelon than the supported command.

COUNTER-GEOINT ANALYSIS

5-21. This type of analysis requires the analyst to have an in-depth knowledge of the supported commander's plans, intentions, and proposed AO as far in advance of commitment as possible. The analyst must have access to all available data and intelligence on threat GEOINT methodology, systems, and processing as well as in-depth information on commercial satellite systems and their availability to the foreign consumer.

5-22. The analyst attempts to define the specific imagery platform deployed against U.S. forces and the cycle involved (time based) from time of imaging through analysis to targeting. Knowledge of threat intelligence cycle to targeting is critical in developing countermeasures to defeat, destroy, or deceive threat

GEOINT. For ground-based, HUMINT-oriented GEOINT (video cassette recorders, digital video recorders), cellular phone cameras, news media organizations) the CI team will be required to collect the data for the analyst.

5-23. This type of information cannot be reasonably considered to exist in any current database. However, collection to support CI (over-flights of friendly forces by friendly forces) during identified, critical, and GEOINT vulnerable times will validate other CI findings and justify countermeasures. This "collection" will be of immense value to the analyst and the supported commander in determining what, if anything, threat imagery has captured. It must be done within the established or accepted threat activity cycle.

COUNTER-TECHINT ANALYSIS

5-24. The CI analyst requires TECHINT data collection to support VA and countermeasures evaluation. Validation of vulnerabilities (data collectable by threat TECHINT) and the effectiveness of implemented countermeasures (a before-and-after comparison of electromagnetic signatures and data) will be nearly impossible without active and timely collection as a prerequisite to analysis. The CI analyst requires a comprehensive, relational database consisting of threat TECHINT systems, capabilities, and methodology.

5-25. Ideally, the CI analyst should be able to forecast threat TECHINT activity; however, such predictions must rely upon other CI, HUMINT, SIGINT, and GEOINT collection. Information on threat TECHINT must be readily accessible from specialized intelligence elements to assist in providing comprehensive assessment to the supported command.

COUNTERINTELLIGENCE SUPPORT TO INTELLIGENCE PREPARATION OF THE BATTLEFIELD

5-26. CI supports IPB by providing demographic information, FISS and ITO threat data that impacts the friendly force commander's MDMP. CI input to the IPB process also assists in the targeting process and can result in cross-cueing of other assets to satisfy the CCIRs.

OPERATIONAL PLANNING

5-27. The effectiveness of CI operations depends largely on the planning that precedes the operation. Operational planning includes establishing the role of CI in the operation; integration with combat forces; establishing operational and intelligence reporting architectures; and identifying CI support to assist in establishing information dominance through the execution of CI functions and the denial of information to the adversary. Early in the planning process, the CICA and 2X directs the efforts to obtain information on the FISS and ITO intelligence, sabotage, terrorism, and subversion capabilities.

5-28. This information allows the development of OPSEC, AT and protection measures to protect the tactical advantage and prevent surprise of U.S. forces during predeployment, transit, and engagement. During predeployment planning, the CICA and 2X should develop as much information as possible concerning the FISS and ITO threat to U.S. forces. This allows the CICA and 2X to develop a CI targets list. The CI targets list identifies those personalities, organizations, and installations that must be seized, exploited, or protected to provide information dominance in the operational environment. Once on the ground in the theater AO, the CI targets list will assist in the immediate targeting of FISS and ITO capabilities to negate, mitigate, or degrade the adversary's ability to collect on U.S. forces; develop countermeasures; and plan and target U.S. forces for attack or information exploitation.

PERSONALITIES

5-29. These are persons who are a threat to security, whose intentions are unknown, or who can assist the intelligence and CI efforts of the command. Personalities are grouped into these three categories. For ease in identification, a color code indicates the category. Colors currently in use are black, white, and gray, respectively.

Black List

5-30. The black list is an official CI listing of actual, suspected, or potential enemy collaborators, sympathizers, intelligence agents, and other persons whose presence threatens the security of the friendly forces (see JP 1-02). Black list includes—

- Known or suspected enemy or hostile espionage agents, saboteurs, terrorists, political figures, and subversive individuals.
- Known or suspected leaders and members of hostile paramilitary, partisan, or guerrilla groups.
- Political leaders known or suspected to be hostile to the military and U.S. political objectives or an allied nation.
- Known or suspected officials of enemy governments whose presence in the theater of operations poses a security threat to U.S. forces.
- Known or suspected enemy collaborators and sympathizers whose presence in the theater of operations poses a security threat to U.S. forces.
- Known enemy military or civilian personnel who have engaged in intelligence, CI, security, police, or political indoctrination activities among troops or civilians.
- Other personalities indicated by the G-2 as automatic arrestees. Included in this category may be local political personalities, police chiefs, and heads of significant municipal and national departments or agencies, and tribal or clan leaders.

Gray List

5-31. The gray list contains the identities and locations of those personalities whose inclinations and attitudes toward the political and military objectives of the U.S. cannot be determined based upon current intelligence. Regardless of their political inclinations or attitudes, personalities may be gray listed when they are known to possess information or particular skills required by U.S. forces. These people are the "unknowns." They may be individuals whose political motivations require further exploration before they can be used effectively by U.S. forces. Examples of individuals who may be included in this category are—

- Potential or actual defectors from the hostile cause whose bona fides have not been established.
- Individuals who have resisted, or are believed to have resisted, the enemy government and who may be willing to cooperate with U.S. forces, but whose bona fides have not been established.
- Scientists and technicians suspected of having been engaged against their will in enemy research projects of high technology programs.

White List

5-32. The white list contains the identities and locations of individuals who have been identified as being of intelligence or CI interest and are expected to be able to provide information or assistance in existing or new intelligence areas. They are usually in accordance with, or favorably inclined toward, U.S. policies. Their contributions are based on a voluntary and cooperative attitude. Decisions to place individuals on the white list may be affected by the combat situation; critical need for specialists in scientific fields, and such theater intelligence needs as may be indicated from time to time. Examples of individuals who may be included in this category are—

- Former political leaders of a hostile state who were deposed by the hostile political leaders.
- Intelligence agents employed by U.S. or allied intelligence agencies.

- Key civilians in areas of scientific research, who may include faculty members of universities and staffs of industrial or national research facilities, whose bona fides have been established.
- Leaders of religious groups and other humanitarian groups.
- Other persons who can materially and significantly aid the U.S. political, scientific, and military objectives and whose bona fides have been established.

INSTALLATIONS

5-33. Installations on the CI targets list are any building, office, or field position that may contain information or material of CI interest or which may pose a threat to the security of the command. Installations of CI interest include—

- Those that are or were occupied by enemy espionage, sabotage, or subversive agencies or police organizations, including prisons and detention centers.
- Those occupied by enemy intelligence, CI, security, or paramilitary organizations including operational bases, schools, and training sites.
- Enemy communication media and signal centers.
- Nuclear research centers and chemical laboratories.
- Enemy political administrative headquarters.
- Public utilities and other installations to be taken under early control to prevent sabotage.
- Production facilities, supply areas, and other installations to be taken under control to prevent support to hostile guerrilla and partisan elements.
- Embassies and consulates of hostile governments.

ORGANIZATIONS

5-34. Any group that is a potential threat to the security of the friendly force must be neutralized, rendered ineffective, or exploited for a greater good. Groups or organizations that are of concern to CI during tactical operations include—

- FISS and ITO organizations.
- National and local political parties or groups known to have aims, beliefs, or ideologies contrary or in opposition to those of the United States.
- Paramilitary organizations, including students, police, military veterans, and former combatant groups known to be hostile to the United States.
- Hostile sponsored organizations or groups whose objectives are to create dissension and spread unrest among the civilian population in the AO.

TARGETING PROCESS

5-35. Targeting is the process of selecting targets and matching the appropriate response to them, including operational requirements and capabilities. The purpose of targeting is to disrupt, delay, or limit threat interference with friendly COAs; it requires coordinated interaction between operations and intelligence planning cells. Targeting is based on the enemy's assets that provide him an advantage, friendly scheme of maneuver, and tactical plans. CI support to the targeting process include the development of CI targets list to identify those FISS and ITO persons, organizations, facilities, or installations that must be exploited through raid and capture to gain additional intelligence or neutralization to disable or destroy, negate, mitigate, or degrade the adversary's ability to collect on U.S. forces.

5-36. The CICA and the 2X need a positive way to keep track of the status of CI targets. A CI target list is used to ensure targets are seized, exploited, or controlled in a timely manner. The plan is keyed to the scheme of maneuver and lists targets as they are expected to appear. When more targets appear than can be exploited, a priority list is used to denote which target takes priority.

- Priority one targets—represent the greatest threat to the command. They possess the greatest potential source of information or material of intelligence or CI value. Priority one targets must be exploited or neutralized first.
- Priority two targets—of lesser significance than priority one. They are taken under control after priority one targets have been exploited or neutralized.
- Priority three targets—of lesser significance than priority one or two. They are to be exploited or neutralized as time and personnel permit. This might be accomplished through either investigations or operations.

INTELLIGENCE CORROBORATION

5-37. Before commitment of combat power to neutralize priority one targets, intelligence used to identify, locate, and fix those targets should be corroborated through other intelligence sources (US military or Government agencies and HN entities, when applicable) or disciplines (GEOINT, SIGINT, HUMINT).

5-38. This corroboration assists in validating the target and avoids wasted effort and resources of combat forces attempting to neutralize a target that is no longer present, active, or occupied.

COUNTERINTELLIGENCE OPERATIONAL ANALYSIS

5-39. Analysis is also used to help direct and focus CI elements to ensure all information requirements are being answered and to adjust collection focus and operational methodologies to provide better support to the commander. The CICA and the 2X support the C/J/G/S-2 by expanding the CCIRs that can be answered through CI collection into ISR tasks that can be answered by a human source and that can be tasked to a specific collection entity.

5-40. The CICA and the 2X provide this information to support the development of the CI collection plan and its integration into the overarching ISR plan. The CICA normally establishes a list of prioritized standing indicators, and supplements this with ISR tasks developed to answer specific CCIRs. The standing indicators are incorporated into the ACE's all-source analysis team's list of indicators that point to a pattern or COA. Each standing indicator is integrated with other indicators and factors so that analysts can detect patterns and establish threat intentions.

COUNTERINTELLIGENCE INTEGRATION INTO THE ISR PLAN

5-41. One of the primary functions of the CICA and 2X is to deconflict CI operations throughout the area of intelligence responsibility and to synchronize all CI assets to eliminate unneeded overlap and duplication of effort or intelligence fratricide. This includes providing input to the ISR plan to integrate CI assets and ensure unity of the intelligence effort among all organic and adjacent CI elements and other intelligence disciplines.

COUNTERINTELLIGENCE OPERATIONAL CONTROL AND GUIDANCE

5-42. The 2X serves as the requirements manager for Army CI and HUMINT entities within their area of intelligence responsibility. Through the use of operational analysis, the 2X can determine what requirements have been answered; identify information gaps and what CI assets and/or documented sources can be tasked to satisfy IRs.

5-43. When a CI team has fulfilled a specific requirement, the 2X can analyze its AO and its active sources and re-direct the team's mission focus to cover information gaps. The2X can also analyze all intelligence

reporting as well as historical information, assessments, and demographics data to develop source profiles that can be provided to CI teams to use for developing new sources of information to answer SIRs.

ANALYTICAL TOOLS

5-44. CI analysis uses tools to archive, fuse, and correlate data to produce analytical products. Some tools can also be used as products themselves to graphically depict information for easier comprehension by the consumer. There are three basic analytical techniques and automated tools that are particularly useful to single-discipline CI analysis. They are the time event chart, matrices, and the link analysis diagram.

5-45. Each of these tools takes fragmented bits of information and organizes them to create a chart or graph that can easily be read. CI collectors and analysts can use automated computer programs such as Analyst's Notebook or Crime Link to produce these tools or they can create them on paper. Computer programs are faster to use than previous methods and have the added advantage of producing a product that can be shared easily and rapidly over networks and portals. The diagrams in this chapter represent the tools that can be produced using automated programs.

TIME EVENT CHART

5-46. A time event chart is a method for placing and representing individual or group actions chronologically. It uses symbols to represent events, dates, and the flow of time. Normally, triangles are used to depict the beginning and end of the chart and may be used within the chart to indicate particularly critical events such as an ideological shift or change. Rectangles, used as event nodes, store administrative data and indicate significant events or activities. Drawing an "X" through the event node may highlight noteworthy or important events.

5-47. Each of these symbols contains a sequence number, date (day, month, and year of the event), and may, if desired, contain a file reference number. The incident description written below the event node is a brief explanation of the incident and may include team size and type of incident. Arrows indicate time flow.

5-48. By using these symbols and brief descriptions, it is possible to analyze the group's activities, transitions, trends, and particularly operational patterns in both time and activity. If desired, the event nodes may be color coded to indicate a particular event or type of event to aid in pattern recognition. The time event chart is the best analytical tool for pattern analysis. Figure 5-2 (page 5-10) shows the symbology used to create a time event chart. Figure 5-3 (page 5-10) shows a time event chart as depicted in Analyst Notebook.

MATRICES

5-49. Construction of a matrix is the easiest and simplest way to show the relationships between a number of similar or dissimilar associated items. The items can be anything that is important to a collection effort such as people, places, organizations, automobile license plates, weapons, telephone numbers, or locations.

5-50. In analysis, matrices are often used to identify "who knows whom," or "who has been where or done what" in a clear concise manner. There are two types of matrices used in human analysis: the association matrix, used to determine existence of relationships between individual human beings, and the activities matrix, used to determine connectivity between individuals and any organization, event, address, activity, or any other nonpersonal entity. The graphics involved in constructing the two types of matrices differ slightly, but the principles are identical.

Association Matrix

5-51. An association matrix shows connections between key individuals involved in any event or activity. It shows associations within a group or associated activity. Normally, this type of matrix is constructed in the form of an equilateral triangle having the same number of rows and columns. Personalities must be listed in exactly the same order along both the rows and columns to ensure that all possible associations are correctly depicted. An alternate method is to list the names along the diagonal side of the matrix. This type

of matrix does not show the nature, degree, or duration of a relationship, only that a relationship exists. The purpose of the matrix (see figure 5-4) is to show the analyst who knows whom and who are suspected to know whom. In the event that a person of interest dies, a diamond is drawn next to the deceased's name on the matrix.

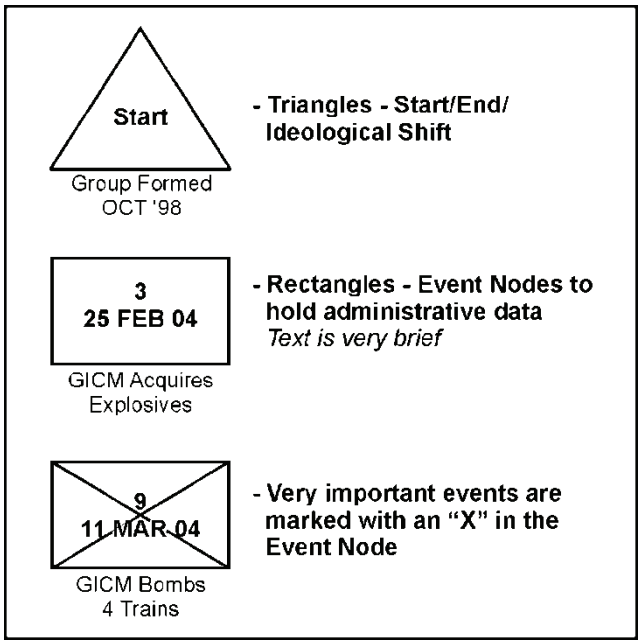

Figure 5-2. Example of a time event chart

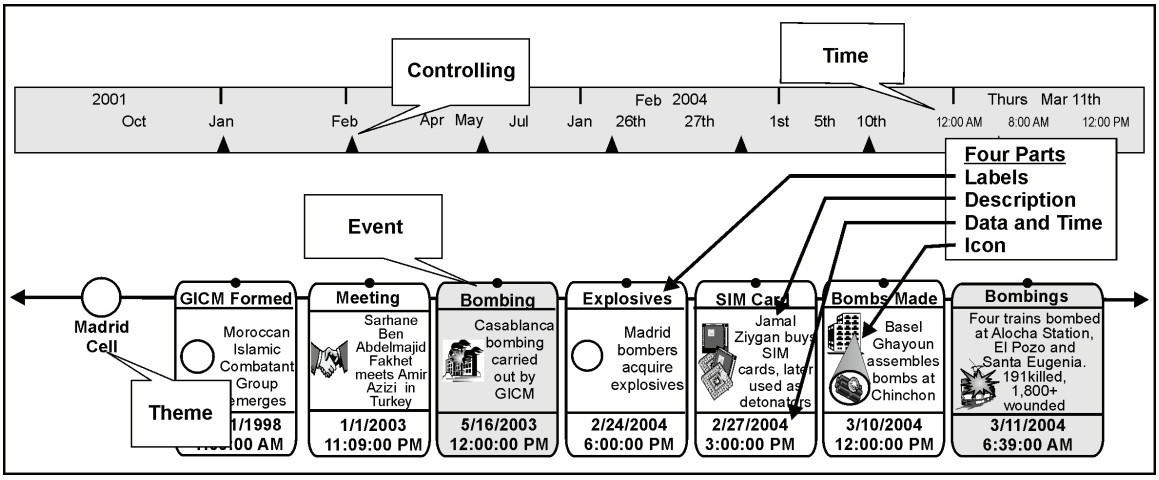

Figure 5-3. Analysis Notebook theme line chart

5-52. The analyst uses a dot or closed (filled-in) circle to depict a strong or known association as shown in figure 5-5. A known association is determined by direct contact between one or more persons. Direct contact is determined by several factors. Direct associations include—

- Face-to-face meetings.
- Telephonic conversations in which the analyst is sure who was conversing with whom.
- Members of a cell or other group who are involved in the same operations.

5-53. Suspected or weak associations in which there are indicators that individuals may have had associations but there is no way to confirm that association; this is depicted with an open circle. Examples of suspected associations are—

- A known party calling a known telephone number (the analyst knows to whom the telephone number is listed), but it cannot be determined with certainty who answered the call.
- A face-to-face meeting where one party can be identified, but the other party can only be tentatively identified.

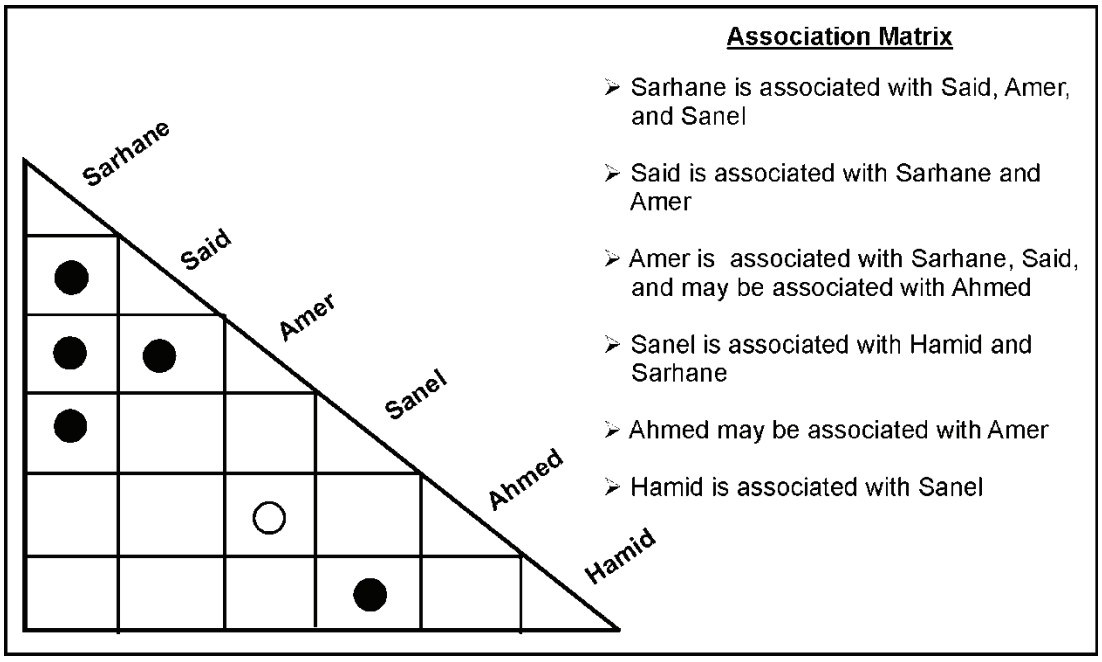

Figure 5-4. Example of an association matrix

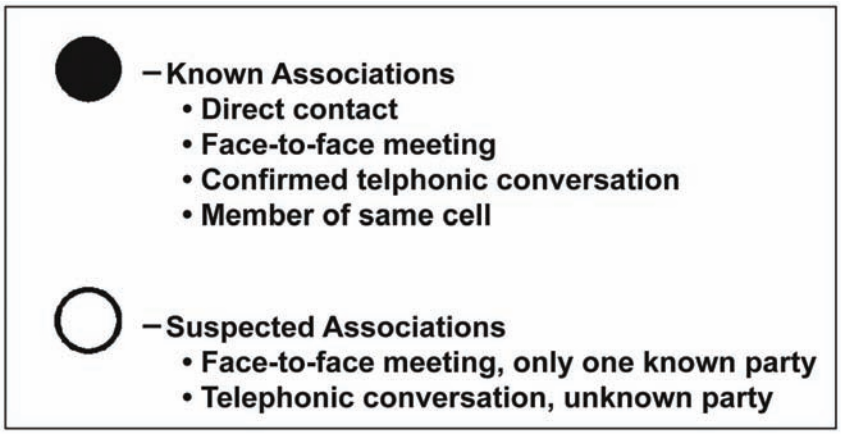

Figure 5-5. Example of an association matrix symbology

5-54. The rationale for depicting suspected associations is to get as close as possible to an objective analytic solution while staying as close as possible to known or confirmed facts. If a suspected association is later confirmed, the appropriate adjustment may be made on the association matrix. A secondary reason for depicting suspected associations is that it may give the analyst a focus for tasking limited intelligence collections assets to confirm the suspected association. An important point to remember about using the

association matrix is that it will, without modification, show only the existence of relationships; not the nature, degree, or duration of those relationships.

Activities Matrix

5-55. Figure 5-6 shows a rectangular array of personalities compared against activities, locations, events, or other appropriate information. The kind and quality of data that is available to the collector determines the number of rows and columns and their content. The analyst may tailor the matrix to fit the needs of the problem at hand or add to it as the problem expands in scope. This matrix normally is constructed with personalities arranged in a vertical listing on the left side of the matrix, with events, activities, organizations, addresses, or any other common denominator arranged along the bottom of the matrix.

5-56. The activities matrix is critical for the study of a group's internal and external activities, external ties and linkages, and even modus operandi. As with the association matrix, confirmed or "strong" associations between individuals and non-personal entities are shown with a solid circle or dot, while suspected or "weak" associations are illustrated by an open circle.

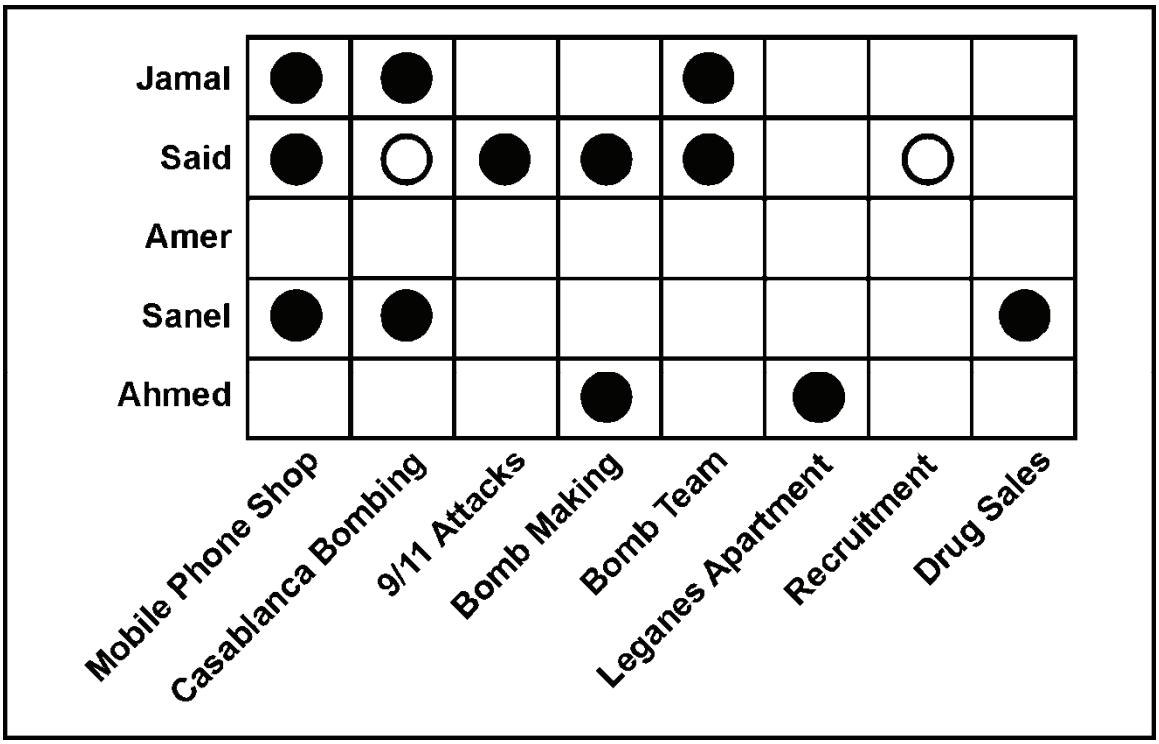

Figure 5-6. Example of an activities matrix

5-57. Using matrices, the analyst can pinpoint the optimal targets for further intelligence collection, identify key personalities within an organization, and considerably increase the analyst's understanding of an organization and its structure. Matrices can be used to present briefings or to store information in a concise and understandable manner within a database. Matrices augment but cannot replace SOPs or standard database files. It is possible, and sometimes productive, to use one matrix for all associations.

LINK ANALYSIS DIAGRAM

5-58. The link analysis diagram shows the connections between people, groups, or activities. The difference between matrices and link analysis is roughly the same as the difference between a mileage chart and a road map. The mileage chart (matrix) shows the connections between cities using numbers to

represent travel distances. The map (link analysis diagram) uses symbols that represent cities, locations, and roads to show how two or more locations are linked to each other. Figure 5-7 is an example of a link analysis diagram.

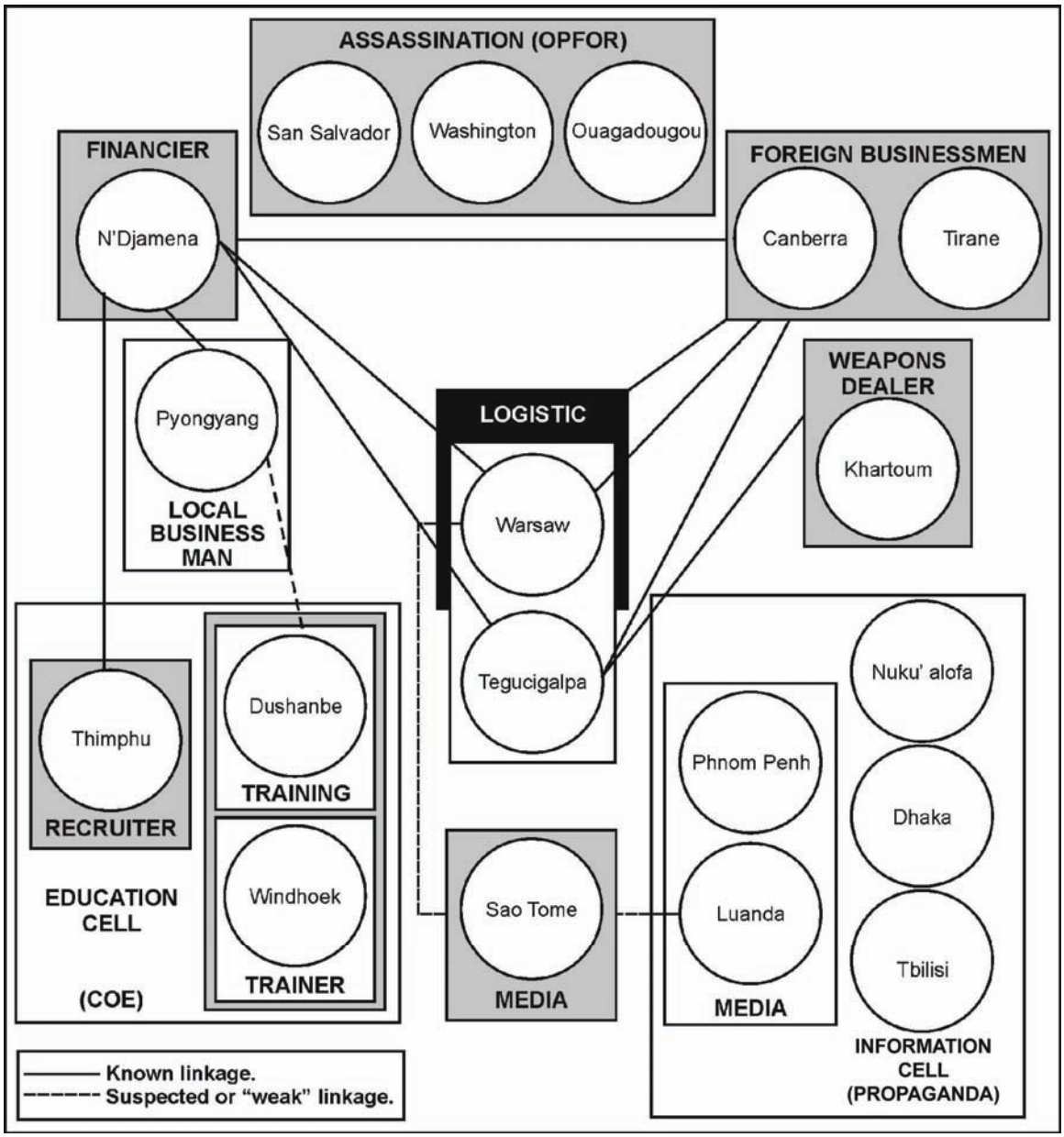

Figure 5-7. Example of a link analysis diagram

5-59. As with construction of association matrices, there are certain rules of graphics, symbology, and construction that must be followed. Standardization is critical to ensuring that everyone constructing, using, or reading a link analysis diagram understands exactly what the diagram depicts. Circles and lines are arranged so that no lines cross whenever possible. Often, especially when dealing with large groups, it is very difficult to construct a line diagram in which no lines cross. In these cases, every effort should be made to keep the number of crossings at an absolute minimum. The standard rules follow.

5-60. Persons are shown as open circles with the name written inside the circle. Deceased persons are depicted in either open circles, with a diamond next to the circle representing that person (as in figure 5-8) or as open diamonds with the name written inside the diamond.

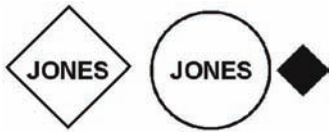

Figure 5-8. Example showing deceased person

- Persons known by more than one name (alias or AKA) are shown as overlapping circles with names in each circle (as shown in figure 5-9) or both names are simply listed in the same circle.

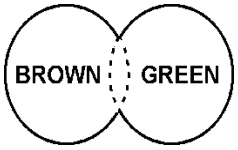

Figure 5-9. Example of person with suspected alias

- If the alias is suspected, a dotted line is used to depict the intersection. If the alias is confirmed, the intersection is shown with a solid line (as shown in figure 5-10).

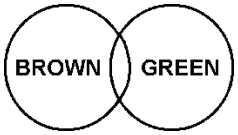

Figure 5-10. Example of person with confirmed alias

- Nonpersonal entities (organizations, governments, events, locations) are shown as appropriately labeled rectangles (as shown in figure 5-11).

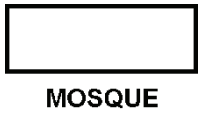

Figure 5-11. Example of nonpersonal entity

- Solid lines (see figure 5-12) denote confirmed linkages or associations.

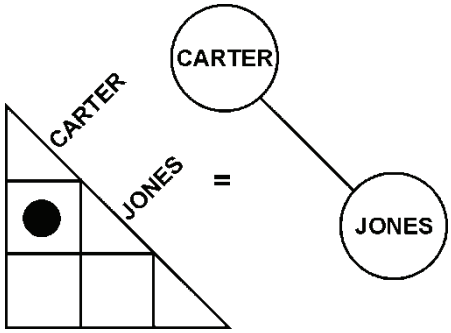

Figure 5-12. Confirmed linkage

- Dotted lines (see figure 5-13) show suspected linkages and associations.

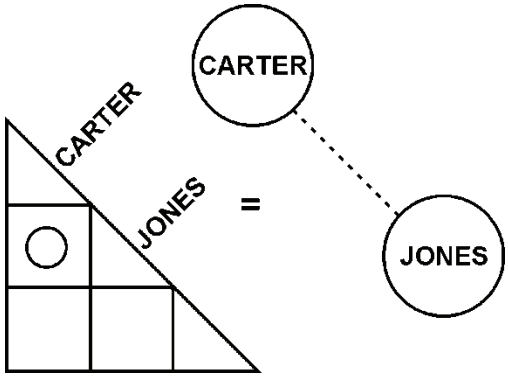

Figure 5-13. Suspected linkage

- Footnotes can be shown as a brief legend on the connectivity line (see figure 5-14).

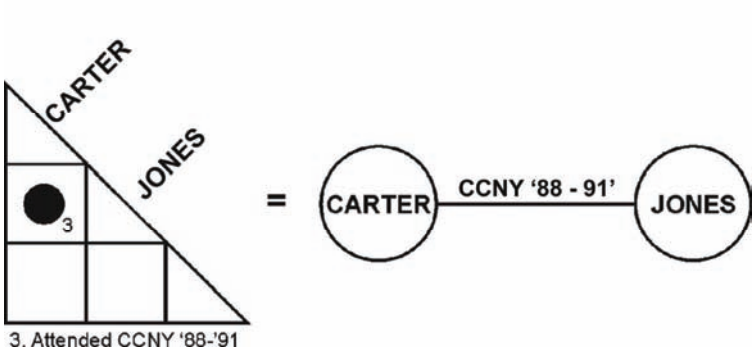

Figure 5-14. Legend on connectivity line

- Each person or non-personal entity is depicted only once in a link analysis diagram. Figure 5-15 shows only connectivity between persons.

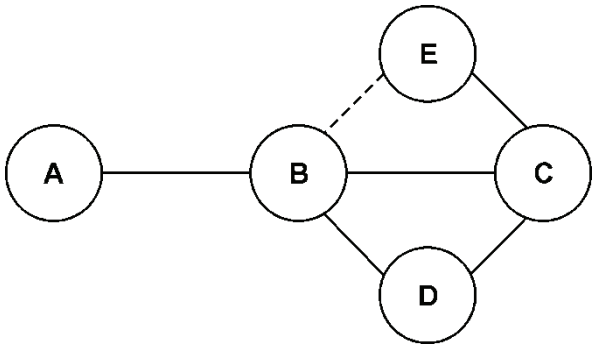

Figure 5-15. Connectivity between persons

5-61. The analyst can easily determine from the diagram that Alpha knows Bravo, Bravo knows Charlie and Delta. Bravo is suspected of knowing Echo, and Charlie knows Delta, Bravo, and Echo. Although the same information could be shown on a matrix, it is easier to understand when depicted on a link analysis diagram. As situations or investigations become more complex, the ease in understanding a link analysis diagram becomes more apparent. In almost all cases, the available information is first depicted and

analyzed on both types of matrices, which are then used to construct a link analysis diagram for further analysis.

5-62. Link analysis diagrams can show organizations, membership within the organization, action teams or cells, or participants in an event. Since each individual depicted on a link analysis diagram can be shown only once, and some individuals may belong to more than one organization or take part in more than one event, squares or rectangles representing non-personal entities may have to overlap.

5-63. Figure 5-16 demonstrates that Ralph and Fred are both members of the "Red Fighters," and that Ralph is also a member of the "Students for Peace." Further, since Ralph and Fred are shown in the same "box," it is a given that they are mutually associated.

5-64. There is more to overlapping organizations than is immediately obvious. At first glance, the overlap indicates only that an individual may belong to more than one organization or has taken part in multiple activities. Further study and analysis would reveal connections between organizations, connections between events, or connections between organizations and events, either directly or through persons. The diagram in figure 5-16 reveals a more complex connection between organizations and personnel.

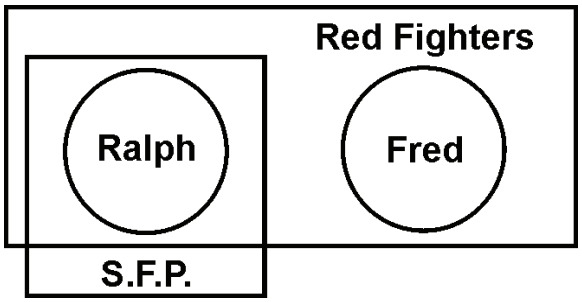

Figure 5-16. Example of mutually associated members

5-65. The analysis diagram in figure 5-17 shows a connection between organizations and events to which an individual belongs or is associated. In this case, a national government runs a training camp for terrorists. Ahmed, a member of the terrorist group, is associated with the training camp, and participated in the bombing attack. From this diagram, one can link the supporting government to the bombing through the camp and the participant.

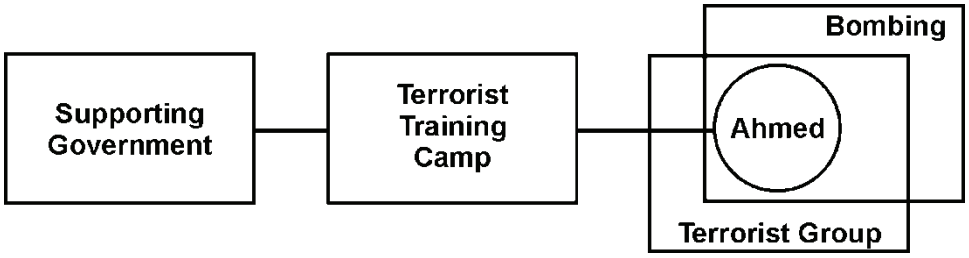

Figure 5-17. Connection between organizations and events

5-66. When, as is often the case, an organization or incident depicted in a link analysis diagram contains the names of more than one individual, it is not necessary to draw a solid line between those individuals to indicate connectivity. It is assumed that individual members of the same cell or participants in the same activity know each other, and the connection between them is therefore implied. If the persons are not mutually associated, they cannot be placed in the same "box." Another solution must be found to depict the situation; that is, show the persons as associated with a subordinate or different organization or activity.

5-67. A final set of rules for link analysis diagrams concerns connectivity between individuals who are not members of an organization or participants in an activity, but who are somehow connected to that entity. Two possibilities exist: First, the individual knows a member or members of the organization, but is not

associated with the organization itself; or second, the person is somehow connected with the organization or activity but cannot be directly linked with any particular member of that entity.

- In the first case, the connectivity line is drawn only between the persons concerned as depicted in figure 5-18.

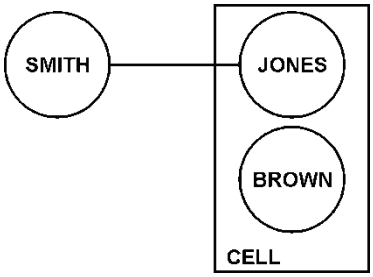

Figure 5-18. Connectivity between persons but not the organization

- In the second case, where Smith is associated with the entity, but not the persons who are members of entity, the situation is shown as depicted in figure 5-19.

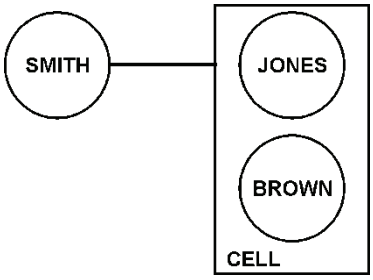

Figure 5-19. Association with an entity

5-68. The steps in constructing a link analysis diagram are as follows:

- **Step 1.** Raw data or fragments of information are organized into logical order. Names of individuals, organizations, events, and locations are compiled on appropriate lists. At this point, a time event chart may be completed to assist in understanding the information and to arrange events into chronological order.
- **Step 2.** Information is entered onto the appropriate matrices, graphically displaying "who is associated with whom" and "who is associated with what."
- **Step 3.** Drawing information from the database and intelligence reports, and relationships from the matrices, the link analysis diagram can be constructed. The best method to start the link analysis diagram is to—
  - Start with the association matrix and determine which person has the greatest number of personal associations. Depict that person in the center of the page (see figure 5-20).

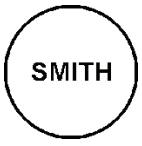

Figure 5-20. Person with greatest number of personal associations

- Determine which person has the next highest number of personal associations. Depict that person near the first person as shown in figure 5-21.

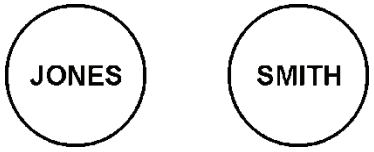

Figure 5-21. Person with next highest number of personal associations

- Use the association matrix and show all confirmed and suspected personal associations (see figure 5-22).

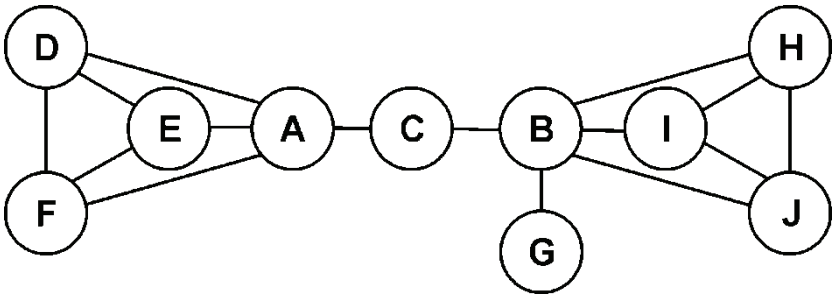

Figure 5-22. Confirmed personal associations

5-69. After all personal associations have been shown on the link analysis diagram, the analyst uses the activities matrix to determine which activities, organizations, or other non-personal entities need to be depicted by appropriate rectangles (as shown in figure 5-23). Having done so, the lines of connectivity between persons within the rectangles may be removed to prevent clutter. (It is assumed that participants in the same activity or members of the same cell are acquainted.)

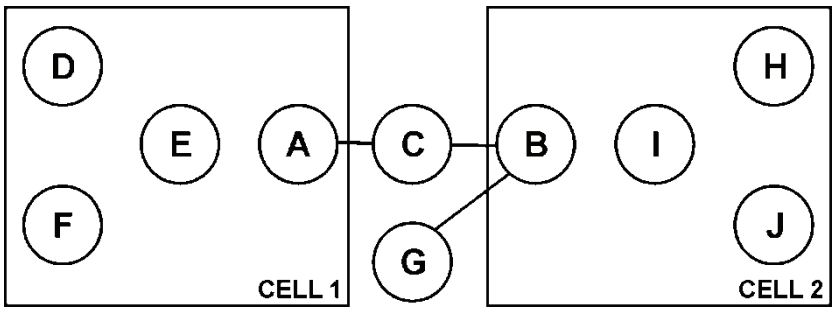

Figure 5-23. Example of activities, organization, and nonpersonal entities

5-70. After completion of the matrices and the link analysis diagram, the analyst makes recommendations about the group's structure, and areas can be identified for further collection. Collection assets are employed to verify suspected connections, ID key personalities, and substantiate or refute the conclusions and assessments drawn from the link analysis that has been done. The link analysis diagram and thorough analysis of the information it contains can reveal a great deal about an organization. It can identify the group's leadership, its strong and weak points, and operational patterns. The analyst can use these to predict future activities. Figures 5-24 through 5-26 show link analysis diagrams and association matrices using Analyst Notebook.

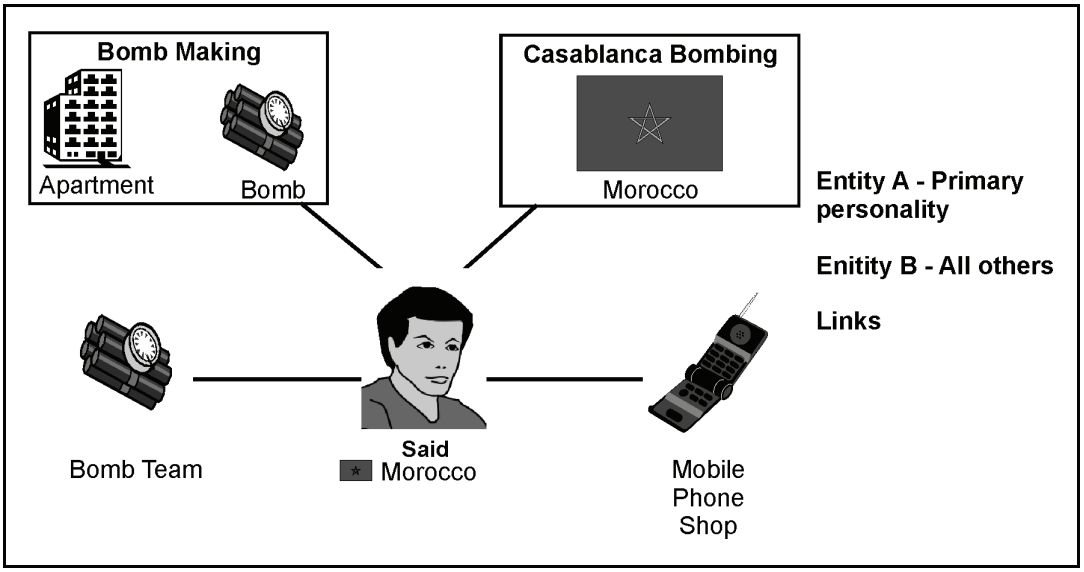

Figure 5-24. Analyst Notebook link diagram showing information from an activity matrix

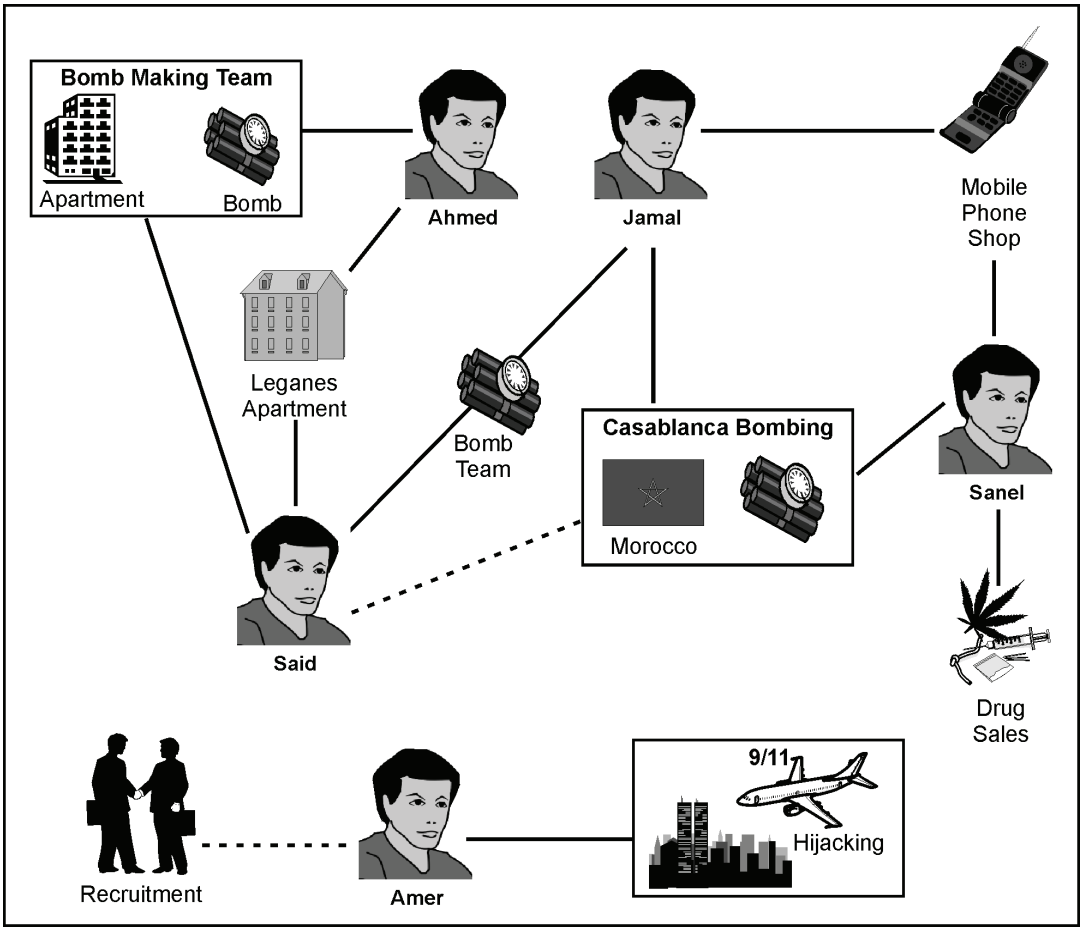

Figure 5-25. Analyst Notebook link diagram showing nonpersonal relationship

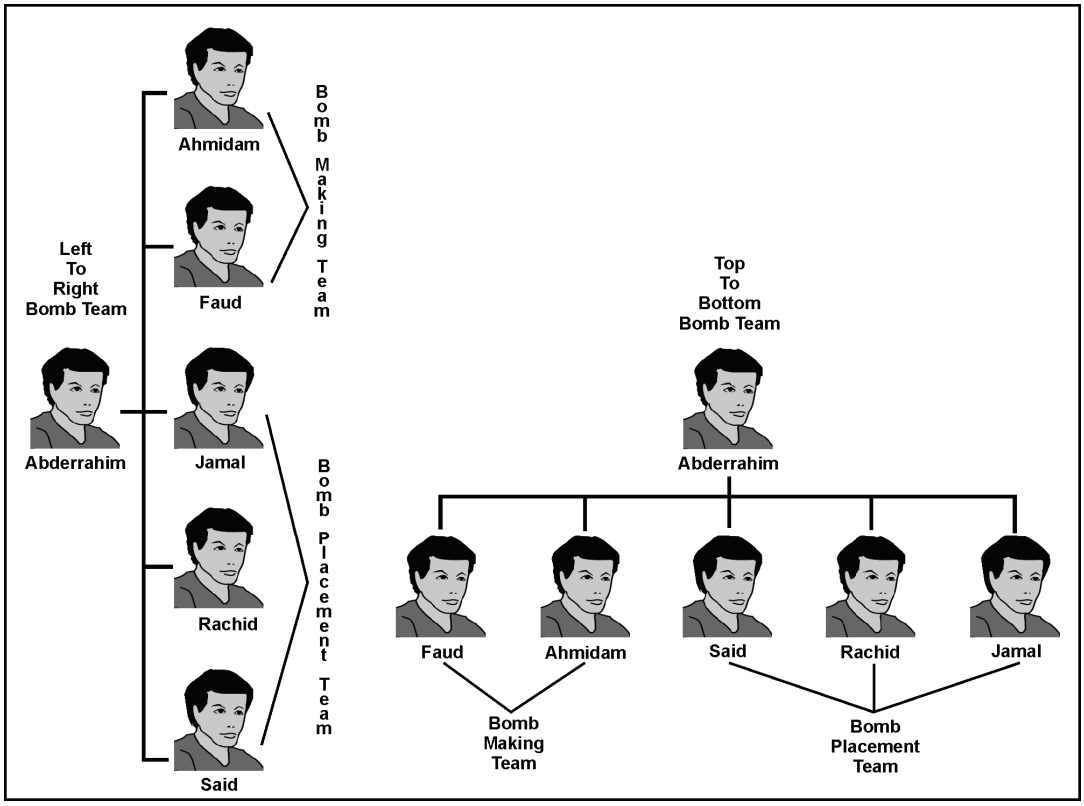

Figure 5-26. Analyst Notebook hierarchy layout

5-71. For more information on other analytical tools, see TC 2-33.4.

PRODUCTION

5-72. CI is an integral part of the IPB process and overall analytical effort. CI is responsible for a variety of products that support the analysis of the adversary's plans, intentions, and capabilities. These products can affect the commander's MDMP or assist in shaping operations of the broader CI mission.

COUNTERINTELLIGENCE ESTIMATE

5-73. The CI estimate is a composite study containing information from each functional area pertaining to a specified contingency area. It is a dynamic document prepared during peacetime and refined and updated continuously. The CI estimate addresses all friendly AOs. The CI estimate contributes to the IPB process. Types of information contained in these estimates vary depending on the contingency area. They generally contain discussions on friendly deployment (including friendly critical nodes) and enemy intelligence collection capabilities and operations (such as sabotage or unconventional warfare). The following are examples of FISS and ITO information found in an estimate:

- Structure.
- Key personalities.
- Methods of operation.
- Collection capabilities.
- Targeting.

THREAT ASSESSMENT

5-74. A threat assessment is the analysis of the FISS and ITO threat directed towards friendly critical nodes and targets. Some of these friendly targets will be identified almost out of common sense, but others will require a concerted analytical effort. In preparing the CI estimate, the team should first concentrate on identifying friendly critical nodes and targets and then examine the known or potential FISS and ITO threat. It should then evaluate the target with respect to their relative criticality, accessibility, vulnerability, and the potential effect of their destruction or degradation in operational effectiveness.

SOURCE PROFILES

5-75. Source profiling is another analytical technique that incorporates both the IPB process with operations analysis. Source profiling is assessing what type of person can satisfy standing information requirements to support the commander's MDMP. While there are negative connotations associated with "profiling," source profiling is designed to maximize the time and resources of CI teams and prevent fishing expeditions by CI special agents hoping to stumble across a good source of information. Developing a source profile is an operational planning tool that can be developed by CI OMTs to operationally focus CI teams.

5-76. Source and demographic overlays can assist in the development of source profiles. CI elements with source profiles can plan missions to put their team into environments where they are most likely to come into contact with someone who can answer a requirement. Once in that environment, the CI element can rapidly evaluate potential sources during elicitation operations and prioritize those persons who may be a potential source of information. Source profiling must factor in the following variables to identify the optimum source for information requirements satisfaction:

- **Demographics.** What ethnicity, tribal affiliation, age, or profession of a source would be able to satisfy the information requirement based upon the situation and/or AO.
- **Placement.** The proximity of the potential source in relation to the environment where he could potentially obtain the information (geographically, culturally).
- **Access.** The ability of a source to obtain direct or indirect information that satisfies a requirement.
- **Motivation.** The convictions, ideologies, or compensatory incentives that would induce a person to cooperate with and provide information to an Army CI element.
- **Control.** The character traits or attributes of a source that would permit him to respond to direction and proactively assist U.S. forces.

This page intentionally left blank.

Chapter 6

Technical Counterintelligence Services and Support

The conduct of investigations is enhanced significantly by the use of existing and emerging technical procedures and techniques, all of which are designed to simplify and shorten the time required to complete certain investigative tasks while ensuring that all evidence, no matter how seemingly insignificant, is thoroughly evaluated. CI units may have access to personnel skilled in technical investigative techniques from higher supporting echelons as well as from within their own ranks.

TECHNICAL INVESTIGATIVE TECHNIQUES

6-1. Technical investigative techniques can contribute materially to the overall investigation. They can assist in providing the commander with timely, factual information on which to base decisions. Specially trained CI special agents conduct TCI investigations to detect clandestine surveillance systems, use polygraph to detect human deception, and employ computer forensics methodologies to investigate known or suspected foreign intrusions into DOD or Army networks.

6-2. All of these personnel are also trained and experienced CI special agents. With the proper approval, CI special agents may employ, or request the proper agency to employ the following activities:

- Electronic surveillance.
- Investigative photography and video recording.
- Laboratory analysis.
- Polygraph support.
- TSCM.
- Deception identification and detection (biometrics).
- Computer forensics.
- Support to information tasks.

ELECTRONIC SURVEILLANCE

6-3. Electronic surveillance is the use of electronic devices to monitor or record conversations, activities, sound, or electronic impulses. Electronic surveillance requires approval as specified in AR 381-10, chapter 5. Requests for electronic surveillance and concealed monitoring activities conducted to support an approved CI investigation must be processed through the ATCICA for staffing and coordination with the appropriate approval authority based upon the criteria outlined in AR 381-10, chapters 5 and 6. Electronic surveillance activities will only be conducted by organizations approved by DA G-2X to support this type of activity.

INVESTIGATIVE PHOTOGRAPHY AND VIDEO RECORDING

6-4. A photograph or video recording may be valuable as evidence since it presents facts in pictorial form and creates realistic mental impressions. It may present evidence more accurately than a verbal or written description. Photographs permit consideration of evidence which, because of size, bulk, weight, or condition, cannot be brought into the courtroom. Photography and video recording in CI investigations include—

- **Identification of individuals.** CI special agents perform both overt and surreptitious photography and video recording. This is considered concealed monitoring and requires approval specified in AR 381-10, chapter 6.
- **Recording of incident scenes.** Agents photograph overall views and specific shots of items at the incident scene.
- **Recording activities of suspects.** Agents use photography and video recording to provide a record of a suspect's activities observed during surveillance or cover operations. This is considered concealed monitoring and requires approval specified in AR 381-10, chapter 6.

6-5. To qualify as evidence, photographs and video recordings must be relevant to the case. A person who is personally acquainted with the locale, object, person, or thing represented must verify the photograph or video recording. This is usually the photographer. The agent will support photographs and video recordings used as evidence by notes made at the time of the photography. These notes provide a description of what the photograph includes. The notes will contain—

- The case number, name of the subject and the time and date that the photographs or video recordings were taken.
- Technical data, such as lighting and weather conditions and type of film, lens, and camera used.
- Specific references to important objects in the photograph.
- These notes may be retained on a form such as a photo data card.

6-6. Physical surveillance, including photography and video recording, requires approval as specified in AR 381-10, chapter 9.

LABORATORY ANALYSIS

6-7. We must anticipate the use of false documentation and secret writing by foreign intelligence agents in many CI investigations. Detection requires specially trained personnel and laboratory facilities. The CI unit SOP should list how this support is obtained.

POLYGRAPH SUPPORT

6-8. The polygraph examination is a highly structured technique conducted by specially trained CI personnel certified by proper authority as polygraph examiners.

6-9. AR 195-6 covers the polygraph program while AR 381-20 covers intelligence polygraphs and describes general applicability, responsibilities, and use of polygraph, records processing, and selection and training of DA polygraph examiners.

6-10. AR 381-20 authorizes intelligence polygraphs for CI investigations, foreign intelligence and CI operations, access to SCI, exculpation in CI investigations; and CSPE to support certain programs or activities listed in AR 381-20.

6-11. The conduct of the polygraph examination is appropriate, with respect to investigations, only when—

- All investigative leads and techniques have been completed as thoroughly as circumstances permit.
- The subject of the investigation has been interviewed or thoroughly debriefed.
- Verification of the information by means of polygraph is deemed essential for completion or continuation of the investigation.

6-12. Do not conduct a polygraph examination as a substitute for securing evidence through skillful investigation. The polygraph examination is an investigative aid and can be used to determine questions of fact, past or present. CI special agents cannot make a determination concerning an individual's intentions or motivations, since these are states of mind and not fact. However, consider the examination results along with all other pertinent information available. Polygraph results will not be the sole basis of any final adjudication. Intelligence polygraph examinations are conducted to—

- Determine the suitability, reliability, or credibility of agents, sources, or operatives of foreign intelligence or CI operations.
- Determine the initial and continued eligibility of individuals for access to programs and activities authorized CSPE support.

6-13. The polygraph examination consists of three basic phases: pretest, in-test, and post-test.

- During the pretest, appropriate rights advisements are given and a written consent to undergo polygraph examination is obtained from all examinees who are suspects or accused. Advise the examinee of the Privacy Act of 1974 and the voluntary nature of examination. Conduct a detailed discussion of the issues for testing and complete the final formulation of questions to be used during testing.
- During the in-test phase, ask previously formulated and reviewed test questions and monitor and record the examinee's responses by the polygraph instrument. Relevant questions asked during any polygraph examination must deal only with factual situations and be as simple and direct as possible. Formulate these questions so that the examinee can answer only with a yes or no. Never use or ask un-reviewed questions during the test.
- If responses indicate deception, or unclear responses are noted during the test, conduct a post-test discussion with the examinee in an attempt to elicit information from the examinee to explain such responses.

6-14. A polygraph examiner may render one or more of four possible opinions concerning the polygraph examination:

- **No opinion.** This is based on the fact that the examiner did not pose enough questions to make a determination.
- **Inconclusive.** This is based on the fact that the completed test results did not support the ability to make a determination of significant response or no significant response.
- **No significant response (NSR).** This is defined as a judgment by the examiner that the physiological responses of the examinee were indicative of veracity and the Polygraph Quality Control Office (PQCO) supports this conclusion.
- **Significant response (SR).** This is defined as a judgment by the examiner that the physiological responses of the examinee were indicative of deception and the PQCO supports this decision.

6-15. Certain mental or physical conditions may influence a person's suitability for polygraph examination and affect responses during testing. CI special agents should report any information they possess concerning a person's mental or physical condition to the polygraph examiner before scheduling the examination. Typical conditions of concern are—

- Mental disorders of any type.
- Any history of heart, respiratory, circulatory, or nervous disorders.
- Any current medical disorder, including colds, allergies, or other conditions (such as pregnancy or recent surgery).
- Use of drugs or alcohol before the examination.
- Mental or physical fatigue.
- Pain or physical discomfort.

6-16. To avoid such conditions as mental or physical fatigue, do not conduct prolonged or intensive questioning immediately before a polygraph examination. The CI special agent tells the potential examinee to continue taking any prescribed medication and bring it to the examination. Based on information provided by the CI special agent and the examiner's own observations, the polygraph examiner decides whether a person is fit to undergo examination by polygraph.

6-17. When the CI special agent asks a person to undergo a polygraph examination, the person is told that the examination is voluntary and that no adverse action can be taken based solely on the refusal to undergo examination by polygraph. Further, the person is informed that no information concerning a refusal to take a polygraph examination is recorded in any personnel file or record.

6-18. The CI special agent will not attempt to explain anything concerning the polygraph instrument or the conduct of the examination. If asked, the CI special agent should inform the person that the polygraph examiner will provide a full explanation of the instrument and all procedures before actual testing and that all test questions will be fully reviewed with the potential examinee before testing.

6-19. Conduct polygraph examinations in a quiet, private location. The room used for the examination must contain, as a minimum, a desk or table, a chair for the examiner, and a comfortable chair with wide arms for the examinee. The room may contain minimal, simple decorations; must have at least one blank wall; and must be located in a quiet, noise-free area. Ideally, the room should be soundproof. Visual or audio monitoring devices may be used during the examination; however, the examiner must inform the examinee that such equipment is being used and if the examination will be monitored or recorded in any manner.

6-20. Normally only the examiner and the examinee are in the room during examination. When the examinee is an accused or suspect female and the examiner is a male, a female witness must be present to monitor the examination. The monitor may be in the examination room or may observe through audio or visual equipment if such is available.

6-21. On occasion, the CI special agent must arrange for an interpreter to work with the examiner. The interpreter must be fluent in English and the required language, and have a security clearance appropriate to the classification of material or information to be discussed during the examination. The interpreter should be available in sufficient time before the examination to be briefed on the polygraph procedures and to establish the proper working relationship.

6-22. AR 195-6 describes polygraph reports, records to be maintained, and records distribution. The CI special agent must provide the examiner with all files, dossiers, and reports pertaining to the investigation or operation before the examination and must be available to answer any questions the examiner may have concerning the case.

6-23. The CI special agent will not prepare any agent reports concerning the results of a polygraph examination. This does not include information derived because of pre-test or post-test admissions, nor does it include those situations where the CI special agent must be called upon by the examiner to question the subject concerning those areas which must be addressed before the completion of the examination.

6-24. The polygraph examiner will prepare a polygraph examination report detailing the facts and circumstances of the examination. A copy of the report may be provided to the CI special agent. Such copies must be destroyed within three months following completion of the investigation or operation. The

original report will be forwarded to and maintained by the U.S. Army Investigative Records Repository (USAIRR), Fort Meade, MD. Request polygraph support in accordance with INSCOM Pamphlet 381-6.

TECHNICAL SURVEILLANCE AND COUNTERMEASURES PROGRAM

6-25. The Army TSCM contributes to information superiority by preventing, detecting, and neutralizing foreign intelligence and security systems (FISS) and international terrorist organizations (ITO) efforts to gain access to classified national security information and sensitive but unclassified information. TEMPEST refers to the evaluation and control of compromising emanations from telecommunications and automated information systems. TEMPEST countermeasures are designed to prevent FISS and ITO exploitation of compromising emanations by containing them within the space of the equipment or facility processing classified information.

6-26. TSCM is concerned with the intentional effort to gather intelligence by foreign intelligence activities by inserting covert or clandestine devices into a U.S. facility, or by modifying existing equipment within that area. For the most part, intelligence gained through the use of technical surveillance means information will be accurate, as people are unaware they are being monitored. At the same time, the implanting of such technical surveillance devices is usually a last resort.

6-27. FISS and ITO elements use all available means to collect sensitive information. One way they do this is by using technical surveillance devices, commonly referred to as "bugs" and "taps." Such devices have been found in U.S. facilities worldwide. Security weaknesses in electronic equipment used in everyday work have also been found worldwide. FISS and ITO easily exploits these weaknesses to collect sensitive or classified conversations as well as the information being processed. They are interested in those things said in (supposed) confidence, since they are likely to reveal future intentions. It should be stressed that vulnerabilities are not just audio, but include video camera signals and data. Devices are usually placed to make their detection almost impossible without specialized equipment and trained individuals.

6-28. The purpose of the TSCM program is to locate and neutralize technical surveillance devices that have been targeted against U.S. Government sensitive or secure areas. The TSCM program includes all measures taken to reduce the technical surveillance threat. The secondary, and closely interrelated purpose, is to provide commanders and department heads with a comprehensive evaluation of their facilities' technical and physical security postures. The Director of Central Intelligence established the requirement for a comprehensive TSCM program. Indoctrination of personnel concerning the technical surveillance threat and the role of the individual in the success of the TSCM program is key.

6-29. The TSCM program includes four separate functions, each with a direct bearing on the program:

- **Detection.** TSCM investigations are designed to detect the presence of technical surveillance devices, technical security hazards, or physical security weaknesses that would permit the loss of sensitive information.
- **Nullification.** Nullification includes both passive and active measures used to neutralize or negate devices that are found. An example of passive nullification is soundproofing. However, soundproofing that covers only part of a room is not very helpful. Excessive wires must be removed, as they could be used as a transmission path from the room. Nullification also refers to those steps taken to make the emplacement of technical surveillance systems as difficult as possible.
- **Isolation.** This refers to the establishment of special areas for the conduct of activities involving sensitive information, and the exclusion or close control of all uncleared personnel. Isolation may involve the designation of a smaller special area with appropriate physical and other security barriers or the isolation of an entire building.
- **Education.** Individuals must know the FISS and ITO threat and their responsibilities before a technical surveillance device is detected or suspected. Additionally, people need to be alert to

what is going on in and around their area, particularly during construction, renovations, and installation of new equipment.

6-30. The TSCM program consists of CI technical investigations and services (such as surveys, inspections, preconstruction advice and assistance) and technical security threat briefings. TSCM investigations and services are highly specialized CI investigations and are not to be confused with compliance-oriented or administrative services conducted to determine a facility's implementation of various security directives.

TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY

6-31. This is an all-encompassing investigation. This investigation is a complete electronic, physical, and visual examination to detect clandestine surveillance systems. A by-product of this investigation is the identification of physical and technical security weaknesses, which could be exploited by FISS and ITO.

TECHNICAL SURVEILLANCE COUNTERMEASURES INSPECTION

6-32. Normally, once a TSCM survey has been conducted, it will not be repeated. If TSCM personnel note several technical and physical weaknesses during the survey, they may request and schedule an inspection at a later date. In addition, they will schedule an inspection if there has been an increased threat posed to the facility or if there is some indication that a technical penetration has occurred in the area. DODD 5240.5 specifically states that no facility will qualify automatically for recurrent TCI support.

6-33. Preconstruction assistance is designed to help security and construction personnel with the specific requirements needed to ensure that a building or room will be secure and built to standards. As with other technical areas, it is much less expensive and more effective to build in good security from the initial stages of a new project. This saves money by precluding costly changes later on.

6-34. Army activities request TSCM support:

- When requesting or receiving support, the facility being inspected must be complete and operational, unless requesting preconstruction advice and assistance. If any new equipment is introduced into the secure area or if access controls are not practiced, the TSCM investigation may be negated.
- Fully justified requests of an emergency nature, or for new facilities, may be submitted at any time, but should be submitted at least 30 days before the date the support is required. Unprogrammed requests will be funded by the requestor. Each request for unprogrammed TSCM support must be accompanied by a funding number to defray the costs of temporary duty (TDY) and per diem.
- The compromise of a TSCM investigation or service is a serious security violation with potentially severe impact on national security. Do not compromise the investigation or service by any action, which discloses to any person, especially one inside the facility, that TSCM activity will be, is being, or has been conducted within a specific area. Unnecessary discussion of a TSCM investigation or service, particularly within the subject area, is especially dangerous because—
  - If a listening device is installed in the area, such discussion can alert persons who are conducting the surveillance and permit them to remove or deactivate their devices. When deactivated, such devices are extremely difficult to locate and may require implementation of destructive search techniques.
  - In the event a TSCM investigation or service is compromised, the TSCM team chief will terminate the investigation or service at once. Report the circumstances surrounding the compromise of the investigation or service to the head of the serviced facility, the appropriate Army command, ASCC, and the INSCOM TSCM program director. TSCM personnel will not reschedule an investigation or service until the cause and impact of the

compromise have been evaluated by the TSCM CI special agent, the appropriate agency head, and the INSCOM TSCM program director.

6-35. When a TSCM surveyor inspection is completed, the requestor is usually given reasonable assurance that the surveyed area is free of active technical surveillance devices or hazards. The TSCM inspector will inform the requestor—

- About all technical and physical security vulnerabilities with recommended regulatory corrective actions.
- That it is impossible to give positive assurance that there are no devices in the surveyed area.
- That the security of the TSCM investigation will be nullified by the admission to the secured area of unescorted persons who lack the proper security clearance.

6-36. The TSCM investigation will also be negated by failing to maintain continuous and effective surveillance and control of the serviced area; allowing repairs or alterations by persons lacking the proper security clearance or not under the supervision of qualified personnel; or introducing new furnishings or equipment without a thorough inspection by qualified personnel.

6-37. Report immediately the discovery of an actual or suspected technical surveillance device via a secure means from a different facility/location. All information concerning the discovery will be handled at a minimum of SECRET. Installation or unit security managers will request an immediate investigation by the supporting CI unit or supporting TSCM element.

DECEPTION IDENTIFICATION AND DETECTION (BIOMETRICS)

6-38. Biometrics as a characteristic is a measurable biological and behavioral characteristic that can be used for automated recognition. Biometrics as a process is an automated method of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

6-39. Identification specific mission areas that CI detection and identification processes and technologies support include, but are not limited to, the following:

- Countering foreign intelligence through the detection, identification, and neutralization of espionage activities.
- Support to military readiness and conduct of military operations through protection, including—
  - Surveillance of air, land, or sea areas adjacent to deployed U.S. forces, sufficient to provide maximum warning of impending attack.
  - Indication of hostile intelligence penetration or attempts at penetration.
- Support to law enforcement efforts to suppress CT.
  - Identification and affiliation of terrorist groups.
  - Assessment of group capabilities, including strengths and weaknesses.
  - Locations of terrorist training camps or bases of operations.
  - Weapons and technologies associated with identified terrorist elements.

IDENTIFICATION

6-40. Biometrics can assist combat units in identifying and tracking the friendly, neutral, and hostile elements within their AO. From a CI perspective, biometrics provides a tool used to identify and database persons during screening operations. CI could also use investigative and forensic activities to obtain fingerprints obtained after a bomb or IED detonation, which may allow for the identification of the bomb maker. This type of intelligence would facilitate targeting and threat negation to support protection, AT, and CT.

6-41. Biometric capabilities are required to identify, database, and track personalities during CI operations and for the conduct of accurate analysis. Biometric signatures would incorporate several physiological criteria (deoxyribonucleic acid [DNA]; voice recognition; and stress, iris, facial, fingerprint data) to significantly enhance intelligence operations and analysis to support protection, AT programs, and CT.

DECEPTION

6-42. Biometric signatures will increase the ability to identify, track, and validate AT and CT intelligence sources through physiological identification and indications of deception. Fingerprint, iris, and facial recognition will be available for fielding to operational units. The system uses—

- A fingerprint scanner, iris scanner, and digital camera for data input.
- Recognition software for identification based on physiological criteria.
- Database software to archive information for recognition and identity comparison.

COMPUTER FORENSICS

6-43. Computer forensics is conducted to—

- Discover and recover evidence related to espionage, terrorism, or subversion against the Army.
- Develop CI investigative leads.
- Collect and report intelligence.
- Support exploitation efforts.

6-44. Processing and examining digital media evidence is a tedious and time-consuming process which requires specialized training and equipment. Failure to properly process and examine digital media evidence could corrupt the evidence or yield the evidence inadmissible during future legal proceedings. Due to the complexities of cyber investigations, computer forensics support to CI investigations will only be conducted by specially trained and qualified personnel assigned to cyber CI elements in each theater.

6-45. Requests for computer forensic support will be made through the appropriate ATCICA. Requests for assistance will include detailed descriptions of the digital media evidence to be seized and examined and will be germane to the approved CI investigative objectives.

6-46. Every CI special agent is responsible for identifying the need for computer forensics support to their investigations. Computer forensics examinations involve a methodical process which, depending on the size and complexity of the digital media evidence, may take a significant amount of time to complete. Computer forensic operations cannot be rushed and therefore investigative time lines may need to be adjusted to accommodate the time required to complete the support. If a CI special agent is in doubt about the capabilities of, or when to leverage, cyber CI units, the agent should contact his ATCICA for guidance.

6-47. Authorized search and seizure activities during an approved CI investigation involving digital media evidence will be conducted by trained and qualified personnel assigned to specific Army intelligence cyber CI units. Some digital media evidence seizures are simple and clear. However, many mobile devices (such

as cell phones and PDAs) that can transmit and receive data, or requires a constant source of power to prevent data loss, require special handling techniques to preserve the evidentiary data.

SUPPORT TO INFORMATION TASKS (COMPUTER NETWORK OPERATIONS)

6-48. The acquisition, possession, management, and control of information are essential to managing the AO. The goal of friendly forces is to achieve information dominance while controlling information the adversary sees, hears, and collects. CNO are critical in establishing information superiority. CNO incorporates defensive information tasks to protect U.S. and coalition information systems while simultaneously executing offensive information tasks to deny, disrupt, and defeat the adversary's information systems. CNO assists the commander in shaping the operational environment and achieving tactical and strategic objectives by affecting the decisionmaking processes of adversarial commanders, combatants, and the civilian populace. Overall, operational continuity and mission success require coordination and synchronization of CNO and intelligence plans and operations to ensure mutual support.

6-49. Army CI includes CI special agents who are technical experts in automation, network operations, Internet technologies, and computer forensics. Cyber CI personnel play a key role in Army CNO initiatives. CI supports CNO by—

- Identifying and analyzing FISS and ITO capabilities that may pose a threat to U.S. automation networks and architecture.
- Examining different applications and software used by an adversary.
- Identifying IP addresses, net users, locations, hardware and peripherals, and artificial constructs.
- Identifying adversary CNO capabilities and providing targeting analysis and planning assistance.
- Conducting TAs and VAs to protect U.S. forces automation networks.

This page intentionally left blank.

Chapter 7

Cyber Counterintelligence

Cyber CI refers to the use of techniques and measures to identify, exploit, or neutralize adversarial operations that use information resources as the primary tradecraft methodology. Cyber CI activities include three primary subdisciplines: computer forensics support to CI investigations, CI network intrusion investigations, and cyber CI operations.

GENERAL

7-1. Cyber CI missions are conducted by specially trained and equipped CI personnel who are assigned to designated cyber CI units. Cyber CI techniques and methods can, and should, be employed in all phases of CI investigations and operations. All CI special agents should know, and plan for the opportunities to leverage cyber CI capabilities in the pursuit of their investigative and operational objectives.

7-2. Like traditional CI activities, cyber CI focuses on countering foreign intelligence and security systems (FISS) and international terrorist organizations (ITO) collection activities targeting information or material concerning U.S. personnel, activities, operations, plans, equipment facilities, publications, technology, or documents, either classified or unclassified, without official consent of designated U.S. release authorities.

CYBER COUNTERINTELLIGENCE SUPPORT TO CORE FUNCTIONS

7-3. The U.S. military's reliance on network centric operations as well as the availability of inexpensive commercial technology to even the smallest of U.S. adversaries has created a significant vulnerability to U.S. military operations. FISS and ITO has increased the targeting of U.S. military networks to collect information, exploit vulnerabilities, and to attack our networks. This threat has resulted in a requirement for specially trained CI special agents who can detect, identify, counter, exploit, or neutralize FISS and ITO threats that occur in cyberspace.

COMPUTER FORENSICS SUPPORT

7-4. Computer forensics support to CI investigations includes the proper seizure, processing, examination, and analysis of digital media evidence to support approved CI investigative objectives. The use of various information systems (including but not limited to computers, networks, mobile computing devices, cellular phones, PDAs) permeates the Army work environment. These information systems, as well as other forms of digital media, are used to store, process, and distribute Army information. These data repositories can easily be concealed and used for data exfiltration, thus potentially making them excellent sources of evidence related to the crime of espionage.

7-5. Processing and examining digital media evidence is a tedious and time-consuming process which requires special training and equipment. Failure to properly process and examine digital media evidence could corrupt the evidence or yield the evidence inadmissible. Therefore, computer forensics support to CI investigations will only be conducted by specially trained and qualified CI special agents. Computer forensics will be conducted by these qualified personnel to—

- Discover and recover evidence related to espionage, terrorism, or subversion against the Army.
- Develop CI investigative leads.
- Collect and report intelligence.
- Support exploitation efforts.

7-6. Requests for computer forensic support will be made through the appropriate ATCICA. Requests for assistance will include detailed descriptions of the digital media evidence to be seized and examined. The requests for assistance will be germane to the approved CI investigative objectives.

7-7. Every CI special agent is responsible for identifying the need for computer forensics support to their investigations. Computer forensics examinations involve a methodical process which, depending on the size and complexity of the digital media evidence, may take a significant amount of time to complete. Computer forensic operations cannot be rushed and therefore investigative time lines may need to be adjusted to accommodate the time required to complete the support.

7-8. Some digital media evidence seizures are simple and clear. However, many mobile devices (such as cell phones and PDAs) that can transmit and receive data or need a constant source of power to prevent data loss require special handling techniques to preserve the evidentiary data.

7-9. If a CI special agent is in doubt about the capabilities of, or when to leverage, cyber CI units, the agent should contact his ATCICA for guidance. All CI special agents will operate in accordance with the appropriate regulations to—

- Ensure that any handling of digital media during CI investigations is performed only by qualified cyber CI special agents or information system specialists.
- Notify or request assistance from properly trained cyber CI special agents as soon as practical after the initiation of an investigation.
- Ensure that their actions are not detrimental to the preservation of digital evidence.

COUNTERINTELLIGENCE NETWORK INTRUSION INVESTIGATIONS

7-10. CI network intrusion investigations involve collecting, processing, and analyzing evidence related to adversarial penetrations of Army information systems. These specialized CI investigations are generally conducted independently of other traditional CI investigations. However, given the jurisdictional issues which involve the Internet, network intrusion investigations may require coordination with other U.S. and foreign government intelligence and law enforcement entities.

7-11. Threats to Army information systems can range from exploitation of vulnerabilities in information systems which allow adversaries to penetrate Army computers and collect critical information, to trusted insiders who either willingly or unwittingly enable adversarial forces to exploit these critical infrastructure resources. Any adversary with the motive, means, opportunity, and intent to do harm poses a potential threat. Threats to Army information resources may include disruption, denial degradation, ex-filtration, destruction, corruption, exploitation, or unauthorized access to computer networks and information systems and data. Cyber CI units are uniquely qualified to investigate and counter these threats.

7-12. All CI network intrusion investigations will be coordinated, to the extent necessary, with the USACIDC, specifically the Cyber Criminal Investigations Unit (CCIU). This coordination is necessary to

ensure that investigative activities are not duplicated and that each organization does not impede or disrupt each other's investigative or prosecutorial options.

7-13. A CI network intrusion investigation may be initiated under, but not necessarily be limited to, the following circumstances:

- Known, suspected, or attempted intrusions into classified or unclassified information systems by unauthorized persons.
- Incidents which involve intrusions into systems containing or processing data on critical military technologies, export controlled technology, or other weapons systems related RDT&E data.
- Intrusions which replicate methods associated with foreign intelligence or adversary collection or which involve targeting that parallels known foreign intelligence or adversary collection requirements.

7-14. The purpose for conducting a CI network intrusion investigation will be to—

- Fully identify the FISS and ITO entity involved.
- Determine the FISS and ITO objectives.
- Determine the FISS and ITO tools, techniques, and procedures used.
- Assist the appropriate authorities with determining the extent of damage to Army and Department of Defense equities.

7-15. If the network intrusion appears to originate from a trusted insider who is under Army jurisdiction and appears to be working for an adversary, the ATCICA or ACICA may authorize an FFI for the purposes of legally prosecuting the subject or to develop the situation to enable neutralization or exploitation of the foreign threat. If it is determined the activity is purely criminal in nature and does not constitute a threat to national security, CI will refer the matter to the appropriate criminal law enforcement organization.

CYBER COUNTERINTELLIGENCE OPERATIONS

7-16. Cyber CI operations rely on cyber mechanisms to collect against, neutralize, or exploit an FISS and ITO threat. Since the FISS and ITO threats to Army information systems are prevalent and very aggressive, cyber CI operations should be designed to assertively counter these pervasive threats.

7-17. Cyber CI units may conduct CI operations in accordance with appropriate regulations to deter, detect, neutralize, and/or support the exploitation of FISS and ITO threats. All proposed cyber CI operations will be documented as a CI special operational concept or CI project and submitted for command and legal endorsement before being forwarded to G-2 for approval.

7-18. The 1st Information Operations Command provides cyber CI elements to support TAs and VAs and red team evaluations. INSCOM provides additional personnel allotments to each theater major subordinate command to provide a dedicated CI LNO to each of the theater regional computer emergency response teams.

7-19. Cyber CI operations include conducting cyber-based collection activities focused on cyber terrorist and foreign intelligence threats that target U.S. interests. In addition to traditional CI collection, which is conducted through the use of sources and other human or multimedia sources, cyber CI collection is primarily conducted via the global information grid to obtain information that impacts the supported unit. Cyber CI collection can result from ongoing CI investigations and/or operations or serve to initiate further CI investigations and/or operations. The goal of cyber CI collection is to provide timely actionable threat intelligence to the supported commander.

Liaison

7-20. Cyber CI elements conduct liaison with U.S., multinational, and HN military and civilian agencies, including NGO, for the purpose of obtaining information of cyber CI interest and coordinating or de-conflicting CI activities. Liaison activities are designed to ensure a cooperative operating environment for cyber CI elements and to develop leads for further exploitation. This is equally true for liaison conducted for cyber CI purposes.

7-21. CI special agents conduct debriefings of friendly force, HN, or the local population who may have information of CI interest regarding adversary intelligence collection or targeting efforts focused on U.S. and multinational interests. Traditional CI special agents conducting this type of collection can provide support to the commander's operational plans and integrated information tasks (information engagement, command and control warfare, information protection, operations security, and military deception), as well as identifying targets for additional cyber collection operations.

7-22. CI special agents work jointly with HUMINT collectors during screening operations to identify civilians in the operational environment, detainees, and other noncombatants who may have information of CI interest to develop leads. During the course of traditional screening operations, if computer software or media is obtained from detainees, cyber CI special agents can be used in a DOMEX role to screen the media for time-sensitive, actionable intelligence information.

Support to Analysis and Production

7-23. CI analysis is used to provide timely, accurate, and relevant all-source assessments regarding the actual and potential foreign intelligence and terrorist threat to DOD, with the objective of protecting DOD personnel, plans, information, research and technology, critical infrastructure, and other national security interest.

7-24. Cyber CI analysis is a uniquely technical discipline. The cyber environment differs from the traditional operational environment in that it is worldwide and "virtual" in nature, not theater specific. In addition to traditional CI analytical work concerning the terrorist and FISS and ITO organizations and operations, it requires detailed technical knowledge of information systems, Army networks, and the global information grid.

7-25. Analysis occurs at all levels from tactical to strategic, but cyber CI analysis is operational and strategic in nature. Because of the uniqueness of the operational environment, and the joint nature of the defenders, cyber CI analysis is conducted by many non-CI activities as well as the Cyber Intelligence Center of the 1st Information Operations Command and the ACIC for the Army.

7-26. At the tactical level, CI teams focus their efforts on supporting mission requirements. These tactical CI teams have a role in providing CI support to all the information tasks. They may provide support to CNO by performing initial incident responder duties when a dedicated cyber CI unit is not available.

7-27. Cyber CI products consist of, but are not limited to, IIRs, target nomination, CI input to TAs and VAs, CI estimates and appendices to OPLANs and OPORDs. Finalized intelligence derived from cyber CI activities may be incorporated into joint and national intelligence databases, assessments, and analysis products, but must be provided in a timely manner to the supported commanders on the ground. Cyber CI production takes place at all levels.

Support to Technical Services

7-28. CI organizations with technically trained cyber CI special agents are chartered with providing unique technical capabilities to augment CI investigations, collection, and operations. These cyber CI technical capabilities are not used as substitutes for traditional CI activities, but support traditional CI techniques employed to counter and neutralize foreign (adversary) intelligence CNO activities.

7-29. In addition to supporting technical CI investigative and operational activities, cyber CI special agents perform highly technical analytical and investigative operations to support Army CNO. Cyber CI special agents are specially trained in the areas of computer operations, network theory and administration, and

forensics, and are instrumental in maintaining U.S. information dominance. The reliance on networked systems will result in greater emphasis being placed on information assurance.

CYBER THREAT BRIEFINGS

7-30. In accordance with AR 381-10 and appropriate regulations cyber threat briefings are a periodic requirement. Cyber threat briefings should—

- Demonstrate CI's understanding of the regulatory purpose and responsibilities regarding cyber issues.
- Be tailored to the audience.
- Identify the cyber threat and what they are targeting.
- Indicate what is reportable.
- Outline responsibilities.
- Provide examples of the cyber threat.
- Seek to influence behaviors of those being briefed.

7-31. A good cyber threat briefing engages the audience, uses mixed media to "grab" the attention of the audience, has easily remembered themes and goals, encourages feedback, and challenges the audience to think like a CI agent. Finally, emphasize the importance of utilizing security patches. Over 90 percent of intrusions into Army networks are due to a lack of patching.

7-32. The trusted insider is the most serious threat to DOD information systems security. The following list of indicators that could be associated with an insider threat should be addressed during threat briefings to CI customers:

- Unauthorized attempts to elevate privileges.
- Unauthorized sniffers.
- Suspicious downloads of sensitive data.
- Unauthorized modems.
- Unexplained storage of encrypted data.
- Anomalous work hours and/or network activity.
- Unexplained modification of network security-related operating system settings.
- Unexplained modification of network security devices such as routers and firewalls.
- Malicious code that attempts to establish communication with systems other than the one which the code resides.
- Unexplained external physical network or computer connection.
- Unexplained modifications to network hardware.
- Unexplained file transfer protocol (FTP) servers on the inside of the security perimeter.
- Unexplained hardware or software found on internal networks.
- Network interface cards that are set in a "promiscuous" or "sniffer" mode.
- Unexpected open maintenance ports on network components.
- Any unusual activity associated with network-enabled peripheral devices, such as printers and copiers.

- Any unusual or unexplained activity focused on transfer devices authorized for moving data across classification boundaries.
- Unexplained attacks appearing to originate from within the local network.
- Attacks against specific network devices, such as intrusion detection systems, originating internal to the local network.
- Unexplained scans for vulnerabilities originating internal to the local network.
- Serious vulnerabilities remaining uncorrected after multiple notifications to the responsible individual to correct the problem.
- Unusual interest in network topologies (firewalls, security hardware or software, inter-site connectivity, trust relationships).
- Unexplained interest in penetration and/or vulnerability testing of the network.
- Unexplained hidden accounts or expected levels of privilege.
- Unauthorized attempts to elevate privileges.
- Attempts to introduce software unapproved for the computing environment.
- Individuals with access displaying undue affluence, unexplained travel, unexplained foreign contacts, unwillingness to take vacation, unwillingness to allow someone to assume their duties, exploitable conduct, abnormal behavior, unexplained and/or extensive technical computer-related knowledge.
- Unauthorized modem connections.
- Encrypted telephonic communication on lines not specifically identified as normally used for encrypted traffic.
- Excessive, unusual, and/or unexplained computer connections over the telephone infrastructure to foreign countries (as identified by traffic analysis or other means).
- Unexplained devices associated with the telephone infrastructure or the connections between the telephone and computing infrastructures.
- Open remote maintenance ports in telephone infrastructure devices.

COMPUTER NETWORK INCIDENT CATEGORIES

7-33. Computer network incidents are identified by category depending on what type of incident occurs. If the incident is deemed a crime, law enforcement takes the investigative lead. If it is determined the incident is of a foreign threat nature, CI will conduct the investigation. The nine categories of computer network-related incidents are listed below:

- **Category 1—Root level intrusion (incident).** Unauthorized privileged access (administrative or root access) to a DOD system.
- **Category 2—User level intrusion (incident).** Unauthorized non-privileged access (user level permissions) to a DOD system. Automated tools, targeted exploits, or self-propagating malicious logic may also attain these privileges.
- **Category 3—Unsuccessful activity attempt (event).** Attempt to gain unauthorized access to the system, which is defeated by normal defensive mechanisms. Attempt fails to gain access to the system (for example, attacker attempt valid or potentially valid username and password combinations), and the activity cannot be characterized as exploratory scanning. Can include reporting of quarantined malicious code.

- **Category 4—Denial of service (incident).** Activity that impairs, impedes, or halts normal functionality of a system or network.
- **Category 5—Noncompliance activity (event).** This category is used for activity that due to DOD actions (either configuration or usage) makes DOD systems potentially vulnerable (for example, mission security patches, connections across security domains, installation of vulnerable applications). In all cases, this category is not used if an actual compromise has occurred. Information that fits this category is the result of non-compliant or improper configuration changes or handling by authorized users.
- **Category 6—Reconnaissance (event).** An activity (scan or probe) that seeks to identify a computer, an open port, an open service, or any combination for later exploitation. This activity does not directly result in a compromise.
- **Category 7—Malicious logic (incident).** Installation of malicious software (for example, Trojan, backdoor, virus, or worm).
- **Category 8—Investigating (event).** Events that are potentially malicious or anomalous activity deemed suspicious and warrants, or is undergoing, further review. No event will be closed out as a category 8. Category 8 will be re-categorized to appropriate categories 1 through 7 or 9 before closure.
- **Category 9—Explained anomaly (event).** Events that are initially suspected as being malicious but after investigation are determined not to fit the criteria for any of the other categories (for example, system malfunction or false positive).

7-34. At a minimum, categories 1, 2, 4, and 7 incidents are reported to DOD law enforcement and/or CI. All incidents involving potential or actual compromise of classified systems or networks are reported through standard CND technical reporting channels.

7-35. AR 25-2 and AR 381-12 outline the commander's requirements for reporting such incidents to law enforcement and CI. Title 18, USC, authorizes those who monitor DOD networks for defensive purposes to share the results of that monitoring with law enforcement and CI. Cyber incident reporting should identify the following relevant information when available:

- Intruder and the victim system.
- Originating IP address and path to the victim system used by the intruder.
- Owner of the originating IP address.
- Date and time of the intrusion and the duration the intruder had access to the victim system. (Use Zulu time.)
- Degree of access obtained by the intruder (for example, user or root level access).
- Classification level, function (for example, web server, domain name server), operating system, and IP address of the victim system.
- Any external security systems, such as ASIM, Netranger, or any other monitoring system—this is done for additional sources—and did the monitoring system detect the activity and alert appropriate personnel.
- The hacking technique used in the incident or intrusion.
- How the technique exploited the victim system (use great detail).
- If the technique exploited a known vulnerability in the information system; if so, provide details about the vulnerability.
- If the system had a security patch or update available that could have prevented the incident and why the patch was not utilized.

- If the technique is being used to target other systems or networks and details about the other victims and systems.
- History of the technique and if it is being used by known hackers or other organizations known to be involved in CNO, including FISS and ITO.
- Results of any inquiry or investigation into the incident.
- Defensive and investigative actions taken in response to the incident.
- Extent of the damage, both actual and potential, caused by the incident.
- Any links between the incident and any previous incidents on DOD systems.
- If the victim has been the victim of previous incidents (provide details).

CYBER INDICATORS OF COUNTERINTELLIGENCE INTEREST

7-36. Unexplained anomalies occur on DOD networks on a daily basis. Some of the anomalies that may be of CI interest are listed below:

- Encrypted data or net flows.
- Unusual login times or failures.
- Unauthorized modification of system files and logs.
- Unauthorized modification of firewall rules.
- Unexplained connectivity—physical or network.
- Anomalous hardware and software.
- Network interface card in “promiscuous” or “sniffer” mode.
- Unusual network traffic on internal network.
- Scanning activity, internal or external.
- Uncorrected vulnerabilities after multiple notifications.
- Unusual interest in network or systems configuration (topologies, firewalls, security measures, trust relationships).
- Unusual interest in penetration or vulnerability testing.
- Unexplained hidden accounts or levels of privilege.
- Attempts to introduce unauthorized software.
- Attempts to obtain an exception to security policy.
- Unauthorized attempts to gain access.
- Attempts to exceed authorized access or elevate privileges.
- Vendor-initiated attempts to install or upgrade hardware or software.
- Unexplained activity of programs or processes.
- Unexplained connectivity of programs or processes.
- Unexplained storage of encrypted files.
- Unauthorized modem connections.
- Excessive, unusual, and/or unexplained foreign connectivity (network or modem).
- Open remote maintenance ports on automated telephone switchboards.

RECOGNIZING POTENTIAL EVIDENCE

7-37. Although CI desires to ultimately exploit a situation to further develop information about adversarial personnel, cells, leadership, and TTP, the opportunity for an arrest or detainment may eventually evolve from any situation, and the proper handling of evidence will play a major role in ensuring prosecution and punishment. Computers and digital media are increasingly involved in cases of espionage and/or terrorism. In these cases, the computer may be contraband, fruits of the crime, a tool of the offense, or a storage container holding evidence of the offense.

7-38. Investigation of any activity that may be of CI interest may produce electronic evidence. Computers and related evidence range from the mainframe computer to the pocket-sized personal data assistant (PDA) to the floppy diskette or CD, a video gaming system, television with built-in recording chip, or the smallest electronic chip device. Images, audio, text, and other data on these media are easily altered or destroyed. It is imperative that CI special agents recognize, protect, seize, and search such devices in accordance with applicable policies, guidelines, and procedures. The following questions need to be answered to determine the role of the computer in relation to the offense:

- Is the computer contraband or fruits of a crime?
- Was the computer software or hardware stolen?
- Is the computer system a tool of the offense?
- Was the system actively used by the accused to commit the offense?
- Were fake IDs or other counterfeit documents prepared using the computer, scanner, or printer?
- Is the computer system only incidental to the offense; that is, being used to store evidence of the offense?
- Is a terrorist using the system to maintain contacts or rosters?
- Is the computer system both instrumental to the offense and a storage device for evidence?
- Did the hacker use the computer to attack other systems and also to store stolen DOD information?

7-39. Once the computer or electronic device role in the offense is understood, the following essential questions need to be answered:

- Is there probable cause to seize hardware?
- Is there probable cause to seize software?
- Is there probable cause to seize data?
- Where will the search be conducted:
  - Is it practical to search the computer system on site or must the examination be conducted at a field office or laboratory?
  - Is it essential for the investigation to do a surreptitious mirror imaging of the hard drive rather than a search and seizure?
  - Considering the massive storage data on today's systems, how will computer forensics experts search the data in an efficient, timely manner?

SEARCH AND SEIZURE

7-40. In preparation for search and seizure of electronic systems, it is essential to keep in mind that using evidence obtained from a seizure in a legal proceeding requires—

- Appropriate collection techniques to avoid altering or destroying evidence.
- Forensic examination of the system completed by trained cyber CI personnel in a timely manner with expert testimony available at trial.

Note. Preparation for search and seizure must include a review of AR 381-10, chapter 7, to determine how to proceed to obtain approval.

7-41. CI special agents must determine if the search warrant or the consent search is more practical for a particular situation.

- The search warrant allows for the search, seizure, and examination of electronic evidence as predefined under the warrant. This method is preferred and consistently is met with the least resistance at the scene and in the courts.
- A consent search and/or seizure allows the individual giving consent an opportunity to withdraw consent at any time during the search and seizure. Continued consent is typically difficult to ensure if the examination process is conducted at a later date and another location. It would be advisable to contact the prosecutor when executing consent searches for computers for this reason.

7-42. Search warrants for electronic storage devices typically focus on two primary sources of information:

- Electronic storage device search warrant (search and seizure of hardware, software, documentation, user notes, and storage media).
- Service provider search warrant (service records, billing records, subscriber information). Request information via appropriate search warrant, subpoena, or court order from a variety of providers (wireless or cellular service, satellite service, electronic data storage, financial institution, Internet, pager).

7-43. Once the computer's role is understood and legal requirements are fulfilled, CI special agents must—

- Secure the scene:
  - Agent safety is paramount.
  - Preserve area for potential evidence and/or fingerprints.
  - Immediately restrict access to computers and attached peripherals. (Keep in mind there are many methods to remotely access computers.)
- Secure the computer as evidence:
  - If computer is off, do not turn it on.
  - If computer is on, consult a computer forensics specialist. If a specialist is not available, photograph the screen, then disconnect all power sources and unplug from the back of the computer. Interrupting power from the back will defeat an uninterruptible power supply.
  - Laptops often have battery power supplies. If the laptop does not shutdown when the power cord is removed, locate and remove the battery pack. The battery is commonly placed on the bottom, and there is usually a button or switch that allows for the removal of the battery. Once the battery is removed, do not return it to or store it in the laptop. Removing the battery will prevent accidental start-up of the laptop.
  - Place evidence tape over each drive slot.
  - Photograph or diagram and label back of computer components with existing connections.
  - Label all connector and cable ends to allow reassembly as needed.

- If transporting is required, package components and transport or store components as fragile cargo.
- Keep away from magnets, radio transmitters, and other potentially damaging elements.
- Collect instruction manuals, documentation, and notes. (User notes may contain passwords.)

- For networked computers, consult a computer specialist for further assistance. Secure the scene and do not let anyone touch the system except personnel trained to handle network systems. Pulling the plug could result in severe damage to the system or network, disruption of legitimate business, or create liability.

7-44. Other electronic devices may contain viable evidence associated with a national security crime of interest to CI. Unless an emergency exits, do not access any device that may be seized. Should it be necessary to access the device, note all actions associated with the manipulation of the device to document the chain of custody and protect the integrity of the evidence.

7-45. Wireless telephones provide users with mobile communications using various protocols and formats (for example, code division multiple access, time division multiple access, global system for mobile) in various frequencies (for example, 900 MHz, 1.2 GHz).

- Potential evidence contained in wireless telephone devices include—
  - Numbers called.
  - Names and addresses.
  - Caller ID for incoming calls.
- Other information contained in the memory of the wireless telephone device include—
  - Phone and pager numbers.
  - Names and addresses.
  - PIN numbers.
  - Voice mail access numbers.
  - Voice mail password.
  - Debit card numbers.
  - Calling card numbers.
  - Email and Internet access information.
  - Service provider information.
  - On-screen image, which may contain other valuable information.
  - A wireless telephone, which may also serve as a PDA.
  - Information on financial and retail transactions.
- If the phone is on, do not turn it off:
  - Turning off the phone could activate a lockout feature.
  - Write down all information on display and photograph if possible.
  - Power down before transport if transport is likely to take so long the device will lose complete battery power.

- If the device is off, do not turn it on:
  - Turning it on could alter evidence on the device.
  - Upon seizure, deliver device to an expert as soon as possible.
  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply.
  - Take appropriate care in the handling and storage (for example, cold or dampness).
  - Anticipate a compulsory process (for example, subpoena) for the service provider to supply additional information.
  - Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-46. Cordless telephones provide users with freedom of movement with the wireless handheld transmitter or receiver as long as the user remains within the range of the telephone base station. The base station serves as the connection between the wireless device and the physical wire connection for telephone service.

- Potential evidence contained in cordless telephone devices include—
  - Numbers called.
  - Numbers stored for speed dial.
  - Caller ID for incoming calls.
- Other information in the memory of cordless telephones include—
  - Phone and pager numbers.
  - Names and addresses.
  - PIN numbers.
  - Voice mail access number.
  - Voice mail password.
  - Debit card numbers.
  - Calling card numbers.
  - On-screen image, which may contain valuable information.
- If the phone is on, do not turn off:
  - Turning off the phone could activate a lockout feature.
  - Write down all information on display and photograph if possible.
  - Power down before transport if transport is likely to take so long the device will lose complete battery power.
- If the device is off, do not turn it on:
  - Turning it on could alter evidence on the device.
  - Upon seizure, deliver device to an expert as soon as possible.
  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply.
  - Take appropriate care in the handling and storage (for example, cold or dampness).

- Anticipate a compulsory process (for example, subpoena) for the service provider to supply additional information.
- Be aware that some home systems are becoming network connected.
- Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-47. Answering machines provide users with a means to capture messages from callers unable to reach the device owner or operator. Some answering machines double as a phone. These devices store messages on tape or in digital memory.

- Potential evidence contained in answering machines include—
  - Incoming and outgoing messages.
  - Home systems are becoming network connected.
  - Numbers called.
  - Numbers stored for speed dial.
  - Caller ID for incoming calls.
  - The same type of information in memory as the cordless phones.
- If the device is on, leave it on:
  - Turning off the device could activate a lockout feature.
  - Some have remote access and must be disconnected from the line as soon as possible (incoming calls can delete evidence).
  - Write down all information on display (photograph if possible).
  - If possible, use a tape recorder to record saved messages.
  - Power down if transport would take so long that device would lose total battery power.
- If the device is off, leave it off:
  - Turning it on could alter evidence.
  - Upon seizure, deliver device to an expert as soon as possible.
  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply.
  - Take appropriate care in the handling and storage (for example, cold or dampness).
  - Anticipate a compulsory process (for example, subpoena) for the service provider to supply additional information.
  - Be aware some home systems are becoming network connected.
  - Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-48. Caller ID devices collect caller information. Often these devices display incoming calls and record established numbers of recent incoming call records.

- Potential evidence contained on caller ID devices include—
  - Telephone and subscriber information from incoming telephone calls.
  - Date and time of incoming calls.

- If the device is on, leave it on:
  - Interruption of the power supply to device may cause loss of data if not protected by internal battery back-up.
  - Document all stored data before seizure or loss of data may occur.
  - Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-49. Electronic paging devices are becoming more sophisticated and some have evolved into two-way messaging systems. The pagers that provide such features receive wireless information and transmit information as well.

- Potential evidence contained in paging devices must be handled carefully.
  - Numeric pagers receive only numeric digits (can be used to communicate numbers and code).
  - Alphanumeric pagers receive numbers and letters and carry full text.
  - Voice pagers transmit voice communications, sometimes in addition to alphanumeric communication.
  - Two-way pagers contain incoming and outgoing messages.
- Once a pager is no longer in proximity to suspect, turn it off.

Note. Continued access to electronic communications over a pager without proper authorization can be construed as unlawful interception of electronic communications (consult legal).

  - Delays in conducting the examination may result in loss of information if power supply becomes insufficient through battery or internal power supply.
  - Take appropriate care in the handling and storage (for example, cold or dampness).
  - May also require service provider search warrant to obtain additional information.
  - Turn it off if necessary.
  - Change batteries if necessary.
  - Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-50. Fax machines provide the user with the ability to transmit documents via phone line from one point to another.

- Fax machines can contain—
  - Speed dial list.
  - Stored faxes (incoming and outgoing).
  - Fax transmission logs (incoming and outgoing).
  - Header line.
  - Clock setting.
- If the fax machine is off, leave it off. If Fax is on, leave it on if possible:
  - Powering down may cause loss of last number dialed and/or stored Faxes—see manufacturer's manual if possible to power down.

- Record saved data before powering off if necessary.
- Take photographs.

- Other considerations regarding Fax machines:
  - Record telephone line number Fax is plugged into.
  - Record network line number Fax is plugged into.
  - Header line should be the same as the phone line (user sets the header line).
  - Some Fax machines are also copiers, scanners, and printers.
  - Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-51. Smart cards and magnetic stripe cards serve many functions, but possess similar characteristics. Both cards interface with a reader device capable of interpreting information stored on the magnetic stripe or computer chip embedded in the plastic card. The most familiar application of these technologies is the credit card. These technologies lend themselves to many additional applications because they are capable of storing any kind of information. These applications include, but are not limited to, driver's licenses, hotel room keys, passports, benefit cards, and security door passes. These technologies can also exist on a card together. (Example uses: point of sale transactions, ATM capabilities.)

7-52. There are two basic types of smart cards:

- First is a memory card which is merely a digital storage device capable of holding large stores of information.
- Second is a microprocessor card which is basically a small computer capable of completing a number of calculations.

7-53. The functionality provided in these cards allows for more robust security in protecting embedded information. The card readers for these cards can also be contact or proximity based. Uses include direct exchange of value between card holders, exchange value over the Internet, storing data or files similar to a computer, wireless telephones, and satellite service devices.

7-54. Magnetic stripe cards can be identified by a black or brown strip that runs across a card. To accurately read the information, magnetic stripe readers must include the capability to read the various tracks. This technology can also be used in a paper or disposable format such as metro passes or parking passes.

7-55. Circumstances raising suspicion concerning smart and magnetic stripe cards include—

- Numerous cards with different names or same issuing vendor.
- Signs of tampering (cards are found in the presence of computer or other electronic devices).

7-56. Questions that must be answered when encountering smart or magnetic stripe cards include—

- To whom is the card issued (valid card holder)?
- Who issued the card?
- What are the uses of the card?
- Why does the person have numerous cards?
- Is there a device or computer present that can alter the card?

7-57. When seizing smart or magnetic stripe cards—

- Photograph the card.
- Label and identify characteristics of the card.

- Detect possible alterations or tampering during initial examination.
- Identify who possessed the card and exactly where it was found (separation from genuine identification and cards may help establish intent).

7-58. ID card printers offer users the ability to print graphics and information onto a plastic card. They can be used to produce counterfeit false identification. ID card printers—

- Contain stored data.
- Should not be powered down if found on unless necessary.
- Should be checked to see if connected to network, are stand alone, or are portable.
- With instruction manuals, power chargers, power cables, and any peripherals belonging to the device should be seized.

7-59. Scanners allow for the creation of a computer image of documents, papers, or items placed on the scanner bed. Some scanners are also copiers, printers, and Fax machines. Scanners—

- Contain stored data.
- Should not be powered down if found on unless necessary.
- With instruction manuals, power chargers, power cables, and any peripherals belonging to the device should be seized.

7-60. Printers allow for the hardcopy creation of items generated by computers. There are many printer technologies including laser, ink jet, thermal dye, and dot matrix. Printers—

- Contain stored data.
- Should not be powered down if found on unless necessary.
- Should be checked to see if connected to network, are standalone, or are portable.

7-61. Other considerations regarding printers:

- Record telephone line number system is plugged into.
- Record network line number system is plugged into.
- Some printers are also copiers, scanners, and Fax machines.
- Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-62. Copiers allow for the duplication of items placed on the copying surface. Copy machines contain—

- Speed dial lists.
- Stored copies (incoming and outgoing).
- Data files (complete images or documents from computers in a network environment).
- Copy transmission logs (incoming and outgoing).
- Header line.
- Clock setting.

7-63. Other considerations for copiers:

- If found on, do not turn off unless necessary.
- Check to see if it is network connected, standalone, or portable.
- Record telephone line number system is plugged into.

- Record network line number system is plugged into.
- Some copiers are also printers, scanners, Fax machines.
- Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-64. Compact disk duplicators and labelers allow for the mass creation of compact disks. When used inappropriately, these devices may be used for sedition and/or subversion support operations.

- Compact disk duplicators and labelers contain stored data.
- If found on, do not turn off unless necessary.
- These systems may be connected to the network, may be standalone, or may be portable.
- Some networked systems contain proprietary hard drives that store images.
- Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-65. Digital cameras, video, and audio media can be recorded as analog or digital information. Many different formats of media are available within both analog or digital. Devices may be standalone, networked, personal, home entertainment, or business (for example, text, still images, graphics, date/time, author, system used).

7-66. Some devices may have basic personal computing functions or may be a computer device itself. Devices are found as portable and fixed devices, but can be easily moved. Devices may store data directly to internal memory and/or removable media. If device is found off, do not turn it on. If found on, consult a specialist.

7-67. If no specialist is available—

- Identify and secure recorded media and media system.
- If recorded media needs to be reviewed immediately, do not pause tape media unless absolutely necessary. Pausing tape media, both video and audio, causes irreversible wear (damage) to the tape resulting in poor image and/or audio quality.
- Immediately secure record tabs on the media to prevent accidental overwrite (recording).

7-68. Securing the system or device:

- Photograph device (screen or display), then disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical.
- Place evidence tape over areas of access (for example, drive slots and media slots).
- Photograph or diagram and label back of components with existing connections.
- Label all connector and cable ends to allow reassembly as needed.
- If transport is required, package components and transport or store components as fragile cargo.
- Conduct examination as soon as possible to avoid possible loss of information if power supply becomes insufficient through battery or internal power supply.
- Take appropriate care in the handling and storage (for example, cold or dampness).
- Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-69. Electronic gaming devices now provide users with greater functionality and are increasingly more comparable with a computer. Electronic gaming devices—

- May contain stored data—text, images, audio, video, other.
- May have Internet access information including emails.
- May contain basic personal computing functions.
- Should not be turned on if found in off position.
- May be found in the on position; in this case, consult a specialist if possible. If a specialist is not available—
  - Photograph device (screen or display), then disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical.
  - Place evidence tape over areas of access (for example, drive slots and media slots).
  - Photograph or diagram and label back of components with existing connections.
  - Label all connector and cable ends to allow reassembly as needed.
  - If transport is required, package components and transport or store components as fragile cargo.
  - Conduct examination as soon as possible to avoid possible loss of information if power supply becomes insufficient through battery or internal power supply.
  - Take appropriate care in the handling and storage (for example, cold or dampness).
  - Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.

7-70. Home electronic devices provide users with a greater degree of interaction with the device. The devices range from interactive television guides to smart kitchen appliances, such as microwaves, that store messages for other family members or refrigerators that keep track of food in its inventory. Home electronic devices—

- May contain stored data (for example, text, images, audio, video, other).
- May contain Internet access information including emails.
- May have telephone capabilities.
- May perform basic personal computing functions.
- May be standalone or networked either at home or through an off-site location.
- Should not be turned on if found in off position.
- May be found in the on position; in this case, consult a specialist if possible. If specialist is not available—
  - Photograph device (screen or display).
  - Play back and record with a tape recorder if device has a readily discernable audio playback feature.
  - Disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical.
  - Place evidence tape over areas of access (for example, drive slots and media slots).
  - Photograph or diagram and label back of components with existing connections.

- Label all connector and cable ends to allow reassembly as needed.
- If transport is required, package components and transport or store components as fragile cargo.
- Conduct examination as soon as possible to avoid possible loss of information if power supply becomes insufficient through battery or internal power supply.
- Take appropriate care in the handling and storage (for example, cold or dampness).
- Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.
- Ensure care is given to the ability of these systems to be remotely accessed. These systems are typically operated through a service provider. Data may not be stored on the system.
- May require a service provider search warrant to obtain additional information.

7-71. GPSs provide users with the ability to locate their position on the Earth's surface by measuring signals transmitted by satellites. These devices assist with navigation and can integrate maps to help users travel from one point to another. GPSs—

- May store data including text, images, and maps.
- May have Internet access information.
- May contain a two-way radio capability.
- May have telephone capabilities.
- May contain routes and marked locations.
- Can keep track of time lines.
- Should not be turned on if found in off position.
- Can be found as an integrated part of other portable devices (for example, palm devices, mini-notebooks, notebook PCs, and digital cameras).
- May be found in the on position; in this case, consult a specialist if possible. If specialist is not available—
  - Photograph device (screen or display), then disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical.
  - Place evidence tape over areas of access (for example, drive slots and media slots).
  - Photograph or diagram and label back of components with existing connections.
  - Label all connector and cable ends to allow reassembly as needed.
  - If transport is required, package components and transport or store components as fragile cargo.
  - Conduct examination as soon as possible to avoid possible loss of information if power supply becomes insufficient through battery or internal power supply.
  - Take appropriate care in the handling and storage (for example, cold or dampness).

- Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.
- Ensure care is given to the ability of these systems to be remotely accessed. These systems are typically operated through a service provider. Data may not be stored on the system.

7-72. PDAs and handheld computers provide users with much of the functionality of full-size personal computers, but are small in size. Palm devices—

- May store data including text, images, and maps.
- May have Internet access information including emails.
- May contain directories.
- May have basic personal computing functions.
- May be standalone or networked within a home or an off-sight location.
- Can keep track of time lines.
- Should not be turned on if found in off position.
- May be found in the on position; in this case, consult a specialist if possible. If specialist is not available—
  - Photograph device (screen or display), then disconnect all power sources; unplug from the back of the device. If unable to do so, recover and consult with a specialist as soon as practical.
  - Place evidence tape over areas of access (for example, drive slots and media slots).
  - Photograph or diagram and label back of components with existing connections.
  - Label all connector and cable ends to allow reassembly as needed.
  - If transport is required, package components and transport or store components as fragile cargo.
  - Conduct examination as soon as possible to avoid possible loss of information if power supply becomes insufficient through battery or internal power supply.
  - Take appropriate care in the handling and storage (for example, cold or dampness).
  - Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.
  - Ensure care is given to the ability of these systems to be remotely accessed. These systems are typically operated through a service provider. Data may not be stored on the system.
  - Keep away from magnets, radio transmitters.
  - May require a service provider search warrant to obtain additional information.

7-73. Security systems are installed as protective measures and are often positioned in strategic locations and can prove to be valuable information for an investigation. Security systems—

- May store data including text, images, and maps.
- May include time stamp information.
- May be standalone or networked via the Internet or a private network.
- Should not be tampered with except by a trained specialist.

- Must be secured. If a specialist is not available, immediately secure recorded data (for example, videotape media) and collect as much of the following information as possible:
  - Make and model.
  - Personal computer-based system or video-based system.
  - Number of cameras.
  - Type of cameras.
  - Locations of system.
  - Location of cameras.
  - Recording media.
  - Media stored and archived.
  - Photographs or video of system.

7-74. Vehicle computer devices provide users with many computer features within their vehicle. They may contain stored data such as text, images, maps, audio, Internet access information, telephone capabilities, routes, marked locations, time lines, and emails. The device can be portable or fixed.

- If the device is found off, do not turn it on. If it is found on, consult a specialist. If a specialist is not available—
  - Photograph the device (screen or display), then disconnect all power sources (unplug from back of device). Most systems are built into the vehicle's interior, integrated into the dash or console areas making it impractical to remove. Actual data may even be stored elsewhere in the vehicle.
  - Place evidence tape over area of access (for example, drive slots and media slots).
  - Photograph or diagram and label back of components with existing connections.
  - Label all connector and cable ends to allow reassembly as needed.
  - Conduct examination as soon as possible to avoid possible loss of information if power supply becomes insufficient through battery or internal power supply.
  - Take appropriate care in the handling and storage (for example, cold or dampness).
  - Seize the instruction manual, power charger, power cables, and any peripherals belonging to the device.
  - Ensure care is given to the ability of these systems to be remotely accessed. These systems are typically operated through a service provider. Data may not be stored on the system. These systems may be integrated with many systems including communications, navigation, security, safety, entertainment, personal computing, Internet, digital audio and imaging into networked environments supported at the home, workplace, public services, and portable devices. They may also require a service provider search warrant to obtain addition information.

7-75. Storage media is used to store data from an electronic device. Some devices have fixed storage space located within the device. This form of storage requires a means of interfacing to another source to transfer the data when necessary. Many devices of today have capabilities for both fixed (internal) storage or memory and the ability to also store data solely or simultaneously to removable storage media. Removable media is used to transfer and store data.

7-76. Some of these media types come in many variations, and there are numerous other types currently in use that are not as prevalent and even more are being introduced into the market on a regular basis.

Although there are some standards, the following list is some of the more common and well-established media types found in the consumer and commercial marketplace:

- Floppy disk.
- Mini-disk.
- Flash memory card.
- External hard drive.
- Digital linear tape.
- High-density floppy disk.
- Compact disk (CD) LS-120 (super disk).
- Click.
- Smart media.
- Micro-drive.
- Digital audio tape.
- Digital video disk.
- Zip.
- Memory stick.
- Removable hard drive.
- Magneto optical drive.

Chapter 8

Investigative Legal Principles

Within the DOD, the controls on intelligence collection activities are set forth in DODD 5240.1 and DOD 5240.1-R. The Army's policy governing intelligence collection activities is AR 381-10, which implements EO 12333 and the DODD and publication.

INTELLIGENCE OVERSIGHT

8-1. Intelligence oversight arises from the same source that created EO 12333. AR 381-10 sets forth the policies and procedures governing the conduct of intelligence collection activities, both by designated Army intelligence components and by personnel not assigned to an intelligence component which conducts intelligence collection activities.

8-2. AR 381-10 does not, in and of itself, authorize intelligence activity—it simply sets forth the policies and procedures for conducting such activities, provided the personnel conducting collection have the appropriate mission and authority. Generally, intelligence oversight applies only to the collection of information on U.S. persons. This does not mean that AR 381-10 is inapplicable when conducting collection against non-U.S. persons; it still applies and sets forth approval authorities for such non-U.S. person collection. Rather than not applying, authority to collect may be granted at a much lower level, in most cases, when conducting collection against a non-U.S. person.

COMPETENCE

8-3. The importance of understanding and complying with these policies cannot be overemphasized. It is imperative that individuals engaged in CI or other intelligence activities read and understand AR 381-10. In particular, they must understand the following concepts:

- The requirement that an Army element must have the mission and authority to conduct specific intelligence activity before a determination is made regarding the ability to collect information on a U.S. person.
- The definition of the terms "collection" and "U.S. person" (chapter 2).
- The retention and dissemination of information about U.S. person (chapters 3 and 4).
- The definitions of special collection techniques and what approvals are required (chapters 5 through 9).
- The definition of questionable intelligence activities, and the reporting of such activities.
- What Federal crimes must be reported, and how.

ROLE OF INTELLIGENCE PERSONNEL IN PROTECTION ACTIVITIES

8-4. AR 381-10 sets forth the role of the SJA as a legal advisor to intelligence personnel. CI special agents should always seek legal advice from their local supporting SJA on the interpretation and application of the procedural guidelines contained in the regulation.

8-5. Agents should rely on a trained lawyer's interpretation when planning to implement any of the special collection procedures.

Basic Understanding

8-6. Because of the nature of their work, CI special agents must understand the basic legal principles. Decisions made by the CI special agent are frequently guided by legal concepts and can have far-reaching implications on the investigation, sometimes very negative.

8-7. Understanding the legal principles allows the CI special agent to recognize potential legal pitfalls and seek assistance before the investigation can be damaged. Only a CI special agent who is familiar with the governing legal principles is able to recognize and conduct these tasks efficiently, and within the parameters of the law.

Requirement

8-8. AR 381-10, chapter 14, states that employees shall conduct intelligence activities only pursuant to and in accordance with EO 12333 and AR 381-10.

8-9. In conducting such activities, employees shall not exceed the authorities granted the employing DOD intelligence components by law, Executive orders including EO 12333, and the applicable DOD and Army directives.

Reporting Questionable Activities

8-10. AR 381-10, chapter 15, requires intelligence employees to report any questionable activity that may be a known or suspected violation of AR 381-10. CI special agents should bear in mind that the definition of questionable activity is very open-ended: any intelligence activity or related activity that might violate any law, any Executive order, any Presidential directive, any applicable DOD policy, or any applicable Army policy.

8-11. Questionable activities must be reported either through command channels or directly to the DA Inspector General (with a courtesy copy to the DA G-2) within 5 work days. CI special agents should look to chapter 15 for specific details on reporting questionable activities.

Reporting Federal Crimes

8-12. AR 381-10, chapter 16, requires intelligence employees to report violations of Federal law, both those committed by intelligence component employees and those committed by non-intelligence employees. With respect to intelligence component employees, any violation of any Federal law must be reported. With respect to non-intelligence component employees, the crimes that must be reported are more limited, and generally focus on crimes involving death or serious bodily injury, or those that constitute a national security crime. Federal crimes should be reported through the chain of command, and must reach DA G-2 within five work days.

Note. In addition to the common crimes, there are additional crimes which may create a conflict for the CI special agent. Unauthorized disclosure of classified material or unauthorized access to information systems by any person, intelligence or not, must be reported. Unfortunately, AR 381-10, chapter 16, directs that such reports go through the chain of command, whereas AR 381-20 and AR 381-12 direct the CI special agent to report a potential CI incident through the ATCICA to the ACICA. In order to protect himself, the CI special agent should note in the remarks section of his report that the incident being reported through the ATCICA to the ACICA is also reportable under AR 381-10, chapter 16, and should be reported to the DA G-2 as such.

JURISDICTION

8-13. Jurisdiction refers to the legal authority of Army CI to conduct investigations of national security crimes or other service-identified incidents of CI interest affecting Army equities. EO 12333 establishes the authority for DOD to conduct CI activities to support DOD missions inside and outside the United States.

Additionally EO 12333 establishes the FBI as the lead agency for CI within the United States and the CIA outside the United States.

8-14. Title 10, USC, establishes the Secretary of Army's authority to write regulations and policy to govern and regulate the activities of the different branches and divisions within the Army, including CI. However, due to the overlap in CI mission areas within the DOD services and other U.S. Government agencies, the 1979 Delimitations Agreement amended in 1996, establishes operational primacy for the different agencies with a CI mission based upon the persons and the incidents involved in a suspected national security crime.

8-15. The Delimitations Agreement was implemented to establish operational boundaries, deconflict CI activities among all CI elements in the intelligence community, and define investigative primacy over specific national security crime incidents. AR 381-20 provides Army specific policy and guidance concerning Army CI missions and activities including investigations and corresponding investigative jurisdiction. AR 381-10 provides detailed policy and guidance on the use, justification, and approval process for special investigative techniques used to support CI investigations. Jurisdiction is derived from two different criteria: jurisdiction over the person and jurisdiction over the incident.

JURISDICTION OVER THE PERSON

8-16. Jurisdiction over the person refers to the persons involved in suspected national security crimes or incidents of CI interest that Army CI may focus investigative efforts to confirm or deny their involvement. Army CI's jurisdiction is limited to persons subject to the UCMJ, with very few exceptions.

8-17. Generally, that jurisdiction is further limited to Army Soldiers, unless DOD has granted Army CI geographic jurisdiction over one or more sister services operating on a specific installation or operating location:

- Jurisdiction over the person within the United States:
  - Active duty Army Soldiers.
  - Retired Army Soldiers who committed the offense while on active duty.
  - Members of the Army Reserve (active or inactive) and the U.S. National Guard, provided the offense occurred while they were on active duty. If the Soldier committed the crime when they were not in a Title 10 status, Army CI will not have jurisdiction over them.
- Jurisdiction over the person outside the United States:
  - Family members of active duty Army personnel.
  - Current DAC employees, including HN DAC employees, and their family members. In some cases, this might also include former DAC employees, depending on whether they committed the incident while employed by the Army.
  - Army contractors and their family members, subject to coordination with the FBI, CIA, and HN. Contractors may or may not be covered by the SOFAs, and their family members are almost never covered. If not covered by the SOFA, the contractor and/or family member is completely subject to HN jurisdiction, even if they are U.S. citizens. However, U.S. citizens that violate Federal criminal law (Title 18, USC) may still be tried in the United States for such violations. This could mean that both the United States and the HN have jurisdiction over the crime.
  - Retirees, Reservists, and National Guard Soldiers regardless of whether they committed the offense while on active duty. However, as with contractors, if the retirees, reservists, or National Guard Soldiers are present in that country in a non-Title 10 status, they are subject to the jurisdiction of that country. Investigations and other actions may require coordination.

- Other U.S. citizens. As above, these individuals are subject to the jurisdiction of the HN, and investigation and other actions require coordination.
- Foreign nationals who are applicants for Army employment or are current or former Army employees are subject to coordination with the HN government. This is a classic example of where the HN may not assist. However, as an example, a German national spying against the U.S. forces in Germany is not violating German law, and unless he is a dual-U.S.-German citizen, he is also not violating U.S. law. As such, while Army CI may have jurisdiction to investigate the actions of that German citizen, the list of post-investigative actions are fairly limited.
- Foreign nationals not associated with the Army, subject to coordination.

JURISDICTION OVER THE INCIDENT

8-18. Jurisdiction over the incident addresses whether or not the incident which occurred is one which the agency in question is permitted to investigate or prosecute. CI incident jurisdiction is laid out in AR 381-20. CI incident jurisdiction includes both crimes under the USC, crimes under the UCMJ, and certain non-criminal incidents that have CI implications.

INVESTIGATIVE AUTHORITY

8-19. If both the persons and the incident involved in a CI investigation are within Army CI jurisdiction, Army CI will have Primary Authority in the investigation. However, if either the person or the incident falls outside Army CI jurisdiction, the case will be a Concurrent or Joint Authority based upon the circumstances of the case. (See AR 381-20, chapter 4, for more details on investigative authorities.)

POSSE COMITATUS ACT

8-20. The Posse Comitatus Act prohibits U.S. military Title 10 forces from acting in a police role within the United States unless approved by Congress. This includes participating in arrests, searches, and seizures of U.S. persons outside the scope of a lawful Army mission. The Posse Comitatus Act does not affect any investigations where Army CI has Primary Authority; however, in Concurrent and Joint Authority cases, it may apply if another civilian LEA is involved due to the circumstances of the case.

CRIMINAL LAW

8-21. Although CI special agents have a fairly limited role in criminal investigations, they must understand the basics of criminal investigations. In many ways CI investigations parallel criminal investigations; they are not the same because they differ in purpose and mandate. That said, however, many of the laws that apply to criminal investigations also apply to CI investigations because they share the same constitutional foundation. Therefore, CI special agents conduct their investigation in such a way that it does not illegally strip away a subject's constitutional rights and result in a dismissal of the case at court-martial.

BEYOND A REASONABLE DOUBT

8-22. In order to secure a conviction against an accused, it is necessary to prove, beyond a reasonable doubt, that the accused committed the crime of which they are accused. Although no numerical standard can be given to this phrase, it can be described as an honest, conscientious doubt based on reason and common sense suggested by the evidence or lack thereof.

8-23. CI special agents understand that the reasonable doubt standard requires more evidence than the "probable cause" standard. Therefore, although CI special agents may only be required to satisfy the probable cause standard, they should work with their unit's assigned SJA to ensure the case is strong enough to withstand the reasonable doubt standard.

PROOF AND ELEMENTS

8-24. Every crime is broken up in terms of "elements." In order to secure a conviction, the government (trial counsels on behalf of) must prove every element of the crime beyond a reasonable doubt. The CI special agent must ensure that they review the elements of the crimes they are investigating, as well as other possible crimes that might apply.

EVIDENCE

8-25. There are several different types of evidence. In terms of their relation to the crime, they are known as direct or circumstantial. In terms of their relation to the world at large, they are known as physical or testimonial:

- **Direct evidence.** Evidence that tends to directly prove or disprove a fact that is in issue (related to an element of the crime).
- **Circumstantial evidence.** Evidence that does not tend to directly prove or disprove a fact in issue, but instead tends to prove or disprove some other fact or circumstance which alone or together with other facts allows the military judge or panel to reasonably infer the existence of the fact in issue. Circumstantial evidence is commonly seen when trying to prove intent or motivation without a confession.
- **Physical evidence.** Any evidence that can be touched or held. Examples include the traditional "smoking gun," a bloody glove, or DNA evidence. From the CI perspective, physical evidence can also include photographs or video surveillance placing the subject at the scene of the dead-drop, the TS documents the subject placed in the dead-drop, or the money the subject later received for those documents.
- **Testimonial evidence.** Confessions and witness statements:
  - In the case of confessions, the Army attempts to use the subject's own words against them. In order to be able to do so, however, it must be evident and proven that their confession was knowing and voluntary, and that they were advised of their right to remain silent. Failure to advise the subject of his rights, or even failure to do so correctly, can result in the subject's confession being inadmissible, and in some cases, may result in other evidence being thrown out as well.
  - In the case of witness statements, the words of another person who witnessed some action are used to prove what happened. While Army CI is not required to advise a witness of his rights, unless they are party to a crime or otherwise admit to committing a crime, the CI special agent must still ensure that the statement is taken correctly. With witnesses, the CI special agent will likely have to prove that they are not biased, that they have no interest in seeing the subject go to jail, that the CI special agent did not pay or coerce them to say what they did, and that they are trustworthy. This does not mean that their statement must be consensual, but when a Soldier is ordered to make a statement, the CI special agent must ensure that such an order is documented.

DEVELOPED EVIDENCE

8-26. This is not, technically speaking, a legally recognized name. It does serve to describe an important type of evidence, however, as it is usually used to refer to evidence that is developed through investigative methods, as opposed to evidence found immediately at the scene of the crime.

INTENT

8-27. A big piece of many criminal acts, including almost all criminal acts within CI jurisdiction, is intent, usually referred to as "specific intent" or "criminal intent." Intent in these circumstances means that the accused either—

- Intended to commit the crime.
- Intended the result of the act.
- Or in some cases, acted in a fashion that was so outrageous that we can say that they should have known what would result.

8-28. While there are some acts that are punishable even without intent, the most serious crimes, and therefore, most serious punishments, almost always require criminal intent.

OTHER EVIDENTIARY CONSIDERATIONS

8-29. In addition to understanding the basic types of evidence, the CI special agent should understand the basics of admissibility, including some of the rules which prevent evidence from being admitted.

Admissibility

8-30. Admissibility of evidence depends primarily on two factors: Is the evidence relevant, and was the evidence obtained legally:

- **Relevance.** The Manual for Courts-Martial and Military Rules of Evidence define relevant evidence as any evidence having a tendency to make the existence of any fact of consequence more or less probable than it would be without the evidence. In other words, evidence is relevant when it tends to help prove or disprove an element of the crime.
- **Legally obtained.** Even assuming the evidence is relevant, if it is obtained illegally, it will be barred from court. Legally obtained includes factors such as whether the CI special agent advised the subjects of their rights, whether they received proper approval before conducting the intelligence collection activity, whether the information provided was covered by a privilege, or whether the evidence is barred by "hearsay" or "fruit of the poisonous tree" doctrine.

Note. There are different rules governing admissibility of evidence during administrative proceedings, such as discharge boards. CI investigations will always be conducted using appropriate legal standards and in a manner which would not jeopardize the potential for prosecution. In the event that a court-martial is unfeasible, or the decision is made not to pursue a court-martial, the CI special agent and the SJA will discuss how such decision will affect the investigation. CI special agents should not, by themselves, act in a fashion that could prevent the Government from seeking a court-martial. Such actions, without permission from the court-martial convening authority, could violate the basic rules on intelligence oversight, and may constitute criminal conduct on the part of the CI special agent.

Hearsay

8-31. Generally, when someone witnesses a crime, that person must testify in court against the accused, rather than simply giving a written statement of what they saw. Attempting to use just the written statement is what is known as "hearsay," which means that we are trying to use their written statement to prove "truth." This is commonly seen as a violation of the Constitutional rights of the accused, although there are some exceptions.

8-32. If CI special agents are concerned about getting a witness into the court room, they need to discuss the situation with their SJA as soon as possible. This includes concerns about maintaining the confidentiality of an informant.

"Fruit of the Poisonous Tree" Doctrine

8-33. The idea behind this doctrine is that CI special agents cannot use illegal evidence to obtain legal evidence. Evidence that is obtained illegally will poison other evidence if that secondary evidence were only able to be obtained because of the illegally obtained evidence.

8-34. The most commonly seen variations of this involve a CI special agent's obtaining an illegal confession (failure to advise of rights) which allows Army CI to locate physical evidence that would not otherwise have been found, or a CI special agent who conducts illegal collection (not properly approved, outside the scope of what was approved), which leads to a confession. In both cases, the secondary evidence would almost certainly be held to be inadmissible.

Plain View

8-35. One legal concept that can often assist investigators is known as plain view. This is the idea that the CI special agent is in a location legally and observes evidence of a crime. At that point, the evidence observed may be collected, and will be admissible.

- **Authorized collection.** Plain view can apply in a variety of situations. The obvious one includes observing evidence during an authorized procedure 7 search. Less obvious includes observing evidence during an authorized procedure 5 in which the CI special agent enters the premises to emplace or retrieve electronic surveillance equipment and notices other evidence of a crime.
- **Inspections.** Plain view also applies to contraband located during an authorized inspection, such as an inspection of cars leaving post, a health-and-welfare inspection, or an inspection of all bags entering or leaving a SCIF.
- **Problems with plain view.** While it is likely that the subject will know about the procedure 7 or inspection, it is entirely possible that the subject is unaware of the procedure 5, and the CI special agent likely wishes the subject to remain unaware of the procedure 5.
  - Unfortunately, seizing plain view evidence observed during the procedure 5 may well alert the subject to the fact that someone has been on the premises, and a smart subject may reach the correct conclusion—that they are under investigation—and change their patterns or activities, thus interfering with the investigation.
  - This does not mean that the CI special agent does not collect the evidence, but instead means that the CI special agent should seek advice from the special agent in Charge or ATCICA, as feasible, before actually seizing the evidence. Alternatives include simply taking photographs of the evidence, and setting forth plans to prevent the evidence from being further disseminated.

Collection and Processing of Evidence

8-36. One of the keys to ensuring that evidence, otherwise obtained legally, remains admissible is to ensure that the proper methods of acquisition and processing are used.

- **Collection (acquisition) procedure.** Approval to conduct the intelligence collection activity is only the first step to obtaining evidence legally. The CI special agent will review AR 381-20, AR 195-5, and FM 3-19.13 for guidance on the proper collection of evidence. In addition, the local CID office may provide advice on proper collection. The CI special agent may also contact the SJA office for advice on whether or not a proposed collection method is legal or whether it may interfere with admissibility. These guides will also assist the CI special agent in recognizing evidence associated with security crimes, planning and conducting investigative searches for evidence, processing evidence in accordance with Army regulations, and presenting evidence in a criminal trial.
- **Preservation of evidence.** In addition to properly collecting evidence, it is important that the proper steps be taken to preserve that evidence. This refers not just the physical preservation of evidence that can degrade or change but also to taking steps to ensure that evidence is not tampered with. (See AR 381-20 and FM 3-19.13, chapter 19, for details on managing and controlling evidence.)

RIGHTS AMENDMENT

8-37. According to UCMJ, article 31(b), anyone subject to the UCMJ may not elicit self-incriminating statements from anyone else subject to the manual until that person has been advised of his rights indicated therein. UCMJ, article 31(b), requires the subject to be informed as to the nature of the accusation, that he does not have to make any statements regarding the offense, and that any statements made by him may be used as evidence against him.

CONSTITUTIONAL BASIS

8-38. The Constitutional basis for the Rights Advisement lies with the 5th and 6th Amendments, summarized as "no one may be compelled to testify against themselves; they must be informed of the charges against them; and they are entitled to legal counsel." These rights are often referred to as "Miranda" rights, based on the case of *U.S. v. Miranda*. As a result of Miranda, the U.S. Supreme Court held that LEAs must advise a subject or accused of their rights before conducting an interrogation or interview.

ADMISSIBILITY OF ADMISSIONS

8-39. Rights advisement is critical because a subject's confession or admission, if obtained by unlawful coercion or by inducement likely to affect its truthfulness will be inadmissible. There is no relief from the requirements of UCMJ, article 31(b), and failure to comply will result in the suppression of all statements. The UCMJ reads, "No statements obtained from any person in violation of this article, or through the use of coercion, unlawful influence, or unlawful inducement may be received in evidence against him (her) in trial by court-martial."

BASIC DEFINITIONS

8-40. There are several definitions that are key to understanding rights advisement. The bottom line is that any time someone is held in custody because they are the suspected of a crime, and while in custody they are interrogated by a Government agent, that person must be advised of their rights before being questioned, and they must make a knowing, intelligent, and voluntary waiver of their rights before they can be questioned.

Custody

8-41. These rights do not take effect unless the subject is in custody. Custody is not the same as apprehension, however. Custody simply implies that the subject's freedom of movement has been restricted, that the subject does not feel free to simply walk away at will. This is particularly sensitive in the military, where the requirements of custom and military law require a Soldier of junior rank to remain in

the presence of the NCO or officer (as long as that NCO or officer is senior) until that NCO or officer dismisses them.

8-42. When a witness enters the CI special agent's office, they are generally free to leave. When a subject enters, however, they usually are not free to leave until the CI special agent has obtained basic information about the incident or subject invokes their right to remain silent. In circumstances where the subject is reluctant to speak with Army CI but does not specifically invoke his rights, the CI special agent should contact the SJA for further guidance.

Interrogation

Note. The term interrogation in this FM refers to those types of interviews or situations used to collect data to support a criminal CI investigation. Any reference to interrogation should not be confused with the systematic collection of intelligence information from EPW/detainees during U.S. military operations. Intelligence interrogations are only authorized to be conducted by 35M/351M or personnel trained and certified in accordance with DOD Directive 3115.09 and FM 2-22.3. CI may debrief EPW/detainees to obtain information of CI value.

8-43. Interrogation is any word or action designed or likely to elicit an incriminating response. Interrogation does not have to be in the form of a question-statement, and, in some cases, silence or body language may be enough. The case of *Brewer v. Williams* (1977) was a famous example, in which the arresting officer, sent to pick up Williams (the subject) in another state, was advised that Williams would make a statement in the presence of his attorney. The officer, upon picking up Williams, did not read him his rights and did not ask him any questions. Instead, during the drive back, he simply made statements concerning some of what the police knew, including where the body was believed to have been hidden.

8-44. The officer finished by giving what has since become known as the "Christian Burial Speech" in which he stated that Williams was the only one that could guarantee that the young girl he had killed would receive a proper Christian Burial. At no time did the detective ever ask Williams a question—he simply made statements. However, the statements, and the guilt they created, led Williams to direct the detective to the site where he had hidden the body. Upon review, the courts determined that the detective had violated Williams' 5th Amendment Rights by interrogating him.

Subject/Accused

8-45. Advising someone of their rights is required when the person being questioned is suspected or accused of a crime. If the person is simply a witness, they are not a suspect or accused, and it is not necessary to advise them of their rights. However, during the questioning of a witness or someone not suspected or accused, the person incriminates himself or makes an admission to any crime, the questioning will be stopped and the person will be advised of his rights.

8-46. After the rights advisement, the questioning may continue if the person waives his rights. In cases like this, the CI special agent should also contact the SJA depending upon the nature of the admission. The key here for the CI special agent is simply to ask the question: Do I have probable cause to believe that the individual I am questioning is suspected of committing a crime? If the answer is yes, treat that person as a subject.

8-47. This is not limited to crimes within CI jurisdiction, and it is possible for a CI special agent, while conducting an interview, to destroy another agency's case by failing to advise the subject of his rights when the subject starts to confess to a crime outside CI jurisdiction. CI special agents should be sensitive to this, and if they hear something that sounds like a confession or admission, they should stop and seek advice from the SJA office before continuing with the interview. Part of the interview process also involves advising the person of what they are suspected or accused of doing. This should be fairly specific. If the subject is advised of one crime, but admits to another during the interview, the CI special agent should stop and re-advise the subject on the other crime as well.

Government Agent

8-48. Government agents include any official acting in a law enforcement capacity. This includes the obvious CID, MP, and MP investigators. It also includes CI special agents while conducting CI investigations. Finally, it includes others designated by law or regulation to serve as investigators. In the military, this also includes individuals who act in an official disciplinary capacity, such as NCOs and officers, particularly those in the chain of command.

FAILURE TO ADVISE

8-49. The failure to advise a subject of his rights can have a significant impact on the case against them, particularly in a CI investigation. As discussed above, while some incidents under CI jurisdiction do not require proving intent, the most serious crimes do require proof of intent. The easiest method for proving intent is through a confession. Failing that, intent can be proven circumstantially, but that is considerably more difficult. On top of the difficulties in proving intent, having a confession thrown out may also result in other evidence being held inadmissible, as discussed above.

WAIVER

8-50. As mentioned above, the waiver must be knowing, intelligent, and voluntary. This means that the subjects must understand what they are doing and saying. They cannot be under the influence of any drug (legal or illegal) or under the influence of alcohol. They cannot even be under the influence of medication that impairs their judgment. They must also be old enough to make a waiver—typically 18.

8-51. A waiver is an area that receives intense scrutiny from the courts, and if defense makes a credible argument that the subject did not make a knowing, intelligent, voluntary waiver, it shifts to the Government to prove that it was. If the CI special agent has any reason to believe that the subject is not capable of making a knowing, intelligent, voluntary waiver, including any reason to believe that the subject is under the influence of any drug or alcohol, the CI special agent needs to terminate the interview.

8-52. The CI special agent can work with the unit to have a blood test performed. If the individual appears confused as to his rights or his status, the CI special agent needs to make every reasonable effort to remove the confusion. If the CI special agent is still not comfortable that the subject understands his rights, the CI special agent should stop the interview and seek legal advice. If the CI special agent is satisfied that the subject understands his rights, the CI special agent will have the subject complete the waiver portion of the DA Form 3881.

SUBSEQUENT INVOCATION

8-53. Even assuming the subject waives his rights, he may still invoke them later during the interview or before a future interview. The subject should be read his rights before every interview, just to be certain. If the subject invokes his rights after previously waiving them, the CI special agent must terminate the interview. Failure to terminate may result in the loss of the entire statement. The CI special agent should also not attempt to persuade the subject to continue with the interview.

SPONTANEOUS STATEMENTS

8-54. Spontaneous statements are statements made by a person in a situation in which the person has some freedom of movement, but has not been advised of his rights. In situations where spontaneous statements are made, the CI special agent will stop the interview and advise the person of his rights and attempt to obtain a waiver and statement after the advisement.

COERCION

8-55. Coercion is strictly prohibited in the conduct of all CI investigations and investigative activities to comply with prosecutorial standards ensure legal admissibility. The courts become concerned when the

subjects are put in a position where they may feel compelled to confess or make a statement based upon an atmosphere of duress, futility, or insurmountable disadvantage. Even attempting to "persuade" the subject to confess will usually receive significant scrutiny by courts and may render any statements or confessions inadmissible in criminal proceedings.

METHODOLOGY

8-56. The CI special agent follows a specific methodology when interviewing a subject to ensure the subject's confession or admission is admissible.

- **Forms.** The CI special agent will use the DA Form 3881 as a guide when advising a subject of his rights. CI special agents should never attempt to recite the advisement based on their memory. If the appropriate forms are not readily available, the CI special agent should delay the interview until the forms are available. The CI special agents should keep a copy of the DA Form 3881 printed with their standard case material as a backup.
- **Read verbatim.** The CI special agent should read directly from the form or card, without deviation, every single time. The CI special agent should follow the script, and obtain the necessary initials, as outlined in the step-by-step guide in this manual. Following the same methodology every time helps ensure that statements will be admissible.
- **Tone of voice.** The CI special agent's tone of voice can be important; if the CI special agent advises the subject in a fashion that implies that the rights advisement is a meaningless formality, a court may hold that the subject did not make a knowing, voluntary, and intelligent waiver.
- **Downplaying.** It is also improper to play down the seriousness of the investigation or play up the benefits of cooperating. In short, the CI special agent must not (by words, actions, or tone of voice) attempt to induce the individual to waive his rights. The court would likely hold such actions as contrary to the purpose of the explanation of rights requirement.
- **Deception.** A CI special agent may emphasize the benefits of cooperation with the Government, as long as it is not done in a coercive manner.

RIGHT TO COUNSEL

8-57. If, at any time, the subject indicates that he wishes to consult with counsel, stop the interview, even if the subject has otherwise stated that he is willing to make a statement. If during the waiver process, the subject indicates that he has spoken with counsel about anything in the last 30 days or so, stop the interview and consult with SJA.

8-58. The subject may request counsel at any time; even if waived initially, the subject may still change his mind and request counsel later, just as he may later invoke his right to remain silent. If the subject requests counsel, the CI special agent should contact his local SJA office immediately after terminating the interview. Questions concerning re-opening the interview, whether the subject will have a military or civilian counsel, and the timeframe for obtaining counsel can be answered by the CI special agent's SJA advisor.

ADVICE ABOUT THE RIGHTS

8-59. It is possible that the subject will ask the CI special agent for advice about whether or not he should invoke his rights. While it is not the job of the CI special agent to advise the subject in this fashion, the CI special agent must keep in mind that advising the subject not to seek counsel, or advising the subject to make a statement, may be seen as an attempt to pressure the subject to waive his rights and could result in the statement being inadmissible.

8-60. The CI special agent's best reply will generally be something along the lines of: "If you are not sure about waiving your rights, perhaps you should talk to counsel, and we can talk again afterwards." While

that may seem counterproductive from the investigator's point-of-view, it will protect the admissibility of statements given.

INAPPLICABLE TO PHYSICAL EVIDENCE

8-61. The 5th Amendment, and article 31, only apply to testimonial evidence. They have no application to, and do not restrict the collection of, physical evidence, including fingerprints, blood samples, DNA, handwriting, or voice exemplars based on a standard template. However, the collection of such physical evidence may require other approvals, and the CI special agent should consult with their SJA.

INVESTIGATIVE AUTHORITY

8-62. CI special agents have several different types of authority when conducting CI investigations. This includes standing investigative authority, the authority to conduct a search and seizure, the ability to apprehend or detain a subject, the ability to perform an investigative stop, and the authority to swear a witness or subject to an oath.

STANDING INVESTIGATIVE AUTHORITY

8-63. In accordance with AR 381-20, CI special agents have standing investigative authority allowing them to gather sufficient information about an incident to prepare a concise CI incident report. This authority cannot be exercised past five work days, and in any case terminates once the CI incident report is submitted. SIA includes the authority to—

- Interview the source of the report.
- Conduct local agency checks.
- Collect and retain physical evidence not requiring approval under AR 381-10.
- Debrief returned special category absentees or repatriated POWs.
- Monitor command investigations of security violations.

8-64. Under no circumstances, however, may the CI special agent use SIA to interview the subject without explicit authority from the ACICA.

SEARCH AND SEIZURE AUTHORITY

8-65. CI special agents are authorized to perform search and seizures within U.S. military installations or facilities, in accordance with AR 381-10, AR 190-22, Military Rules of Evidence, and other applicable policies. Such searches or seizures must be properly approved by the appropriate commander or Military Judge. CI special agents may not perform searches or seizures outside DOD installations in the United States, but may, with permission, accompany the civilian LEA (typically the FBI) who is conducting the search or seizure. Off-post searches or seizures outside the United States is governed by AR 381-10 and existing SOFAs.

Constitutional Protection

8-66. U.S. citizens are protected from unreasonable searches or seizures by the 4th Amendment to the Constitution. Additionally, the Uniform Code of Military Justice provides similar protections for Service Members. CI searches are addressed in Procedure 7, AR 381-10. Under no circumstances should a CI special agent attempt to initiate, request or encourage a search outside of Procedure 7 - such a search will likely be held to be illegal, as approval for a CI search requires additional elements that are not present in non-CI searches.

Unlawful Searches

8-67. An unlawful search is one made of a person, a person's house, papers, or effects without probable cause to believe that the person committed a crime within the jurisdiction of the investigating agency, and that evidence of the crime would be found in the area to be searched.

Probable Cause

8-68. Although probable cause applies to more than just searches, searches require an additional type of probable cause—probable cause (reasonable belief based on identifiable and definitive facts) to believe that the particularly described evidence will be found in the particularly described location to be searched. The 4th Amendment does not permit LEAs to simply ransack the house, person, or papers of a U.S. citizen; instead, LEAs must have a specific plan for the conduct of the search to minimize the impact with respect to the Constitutional rights of the person subjected to the search. Probable cause is more than mere suspicion, more than "good reason to suspect," or "I have a hunch." Probable cause requires that the CI special agent can point to facts supporting his belief, such as photographs, statements, or other factual evidence.

Legal Searches

8-69. Generally, a legal search is one authorized by the commander or Military Judge, based on probable cause and evidence. There are a few exceptions, however, that allow searches without requiring probable cause:

- **Consent.** Consent waives any expectation of privacy. The CI special agent may always request consent to conduct a search and, if granted, may conduct the search within the limits of the consent, until consent is withdrawn. If the subject limits the scope of the consent, the CI special agent must comply with those limitations unless he has a separate authorization or warrant. If the subject withdraws consent, the CI special agent must terminate the search unless the CI special agent has a separate authorization or warrant.
- **Search incident to apprehension.** When a subject is apprehended, the CI special agent is permitted to conduct a brief search of the immediate area within the subject's reach. While this is primarily for the safety of the agent, it also allows the agent to locate contraband that could be easily removed or destroyed. This search includes the subject and easily opened containers within "lunging distance." Containers that are locked, or latched in a method that would prevent their being opened easily may not be searched based on apprehension. Lunging distance is not an absolute number, but 15 feet can be used as a general rule. When the subject is apprehended in his automobile, the CI special agent may search the entire passenger compartment, but may not search the engine area or trunk unless the trunk is not separate from the passenger compartment, such as with a hatchback. CI special agents may not conduct searches of off-post quarters in the United States; conducting apprehensions at such quarters may be seen as an attempt to circumvent this rule.
- **Search incident to an investigative stop.** This is similar to a search incident to apprehension, but is more limited. Here the purpose is entirely focused on the safety of the officer, with a very limited exception concerning evidence that can be readily destroyed. Again, the CI special agent may search the subject, including backpacks or purses. If the stop involves a car, but the subject steps out of his car, the CI special agent will not be able to search the passenger compartment. As above, the CI special agent may not conduct searches of off-post quarters in the United States; conducting investigative stops at such quarters may be seen as an attempt to circumvent this rule.

Documentation

8-70. The CI special agent should obtain the search authorization in writing whenever possible. While it is possible to obtain verbal authorization, particularly in a time-critical situation, the verbal authorization should be followed up with a written authorization. Reducing the authorization to writing helps ensure the admissibility of evidence collected. The CI special agent needs to address several factors in the request, including the following, and should consult with the SJA for assistance in drafting and processing the request. Refer to AR 381-10, chapter 7, for more details.

- Identification of the person or description of the property to be searched.
- A statement of facts to show there is probable cause to believe the subject of the search is—
  - Engaged in clandestine intelligence activities, sabotage, international terrorist activities, activities in preparation for international terrorist activities, or conspiring with or knowingly aiding and abetting a person engaging in such activities, for or on behalf of a foreign power.
  - An officer or employee of a foreign power.
  - Knowingly taking direction from or acting in knowing concert with, and thereby unlawfully acting for or at the direction of a foreign power.
  - A corporation or other entity that is owned or controlled directly or indirectly by a foreign power.
  - In contact with, or acting in collaboration with, a foreign intelligence or security service, to provide access to information or material classified by the United States and to which the subject has access.
- A statement of facts to show that the significant foreign intelligence or CI expected to be obtained cannot be gathered by less intrusive means.
- A description of the extent of the search and a statement of facts to show that the search will involve the least amount of physical intrusion to meet the objective.
- A description of the expected dissemination of the product of the search, including the procedures governing the retention and dissemination of incidentally acquired U.S. person information.

Scope of the Search

8-71. A search is limited in scope, as described in the request and subsequent authorization or warrant. The CI special agent must ensure that they stay within the scope of the authorization. Going outside the scope for any reason, regardless of how logical that reason seems, may cause evidence found to be inadmissible. If the CI special agent conducting the search has reason to believe that the scope should be expanded, the CI special agent should stop the search, secure the location, and submit an additional request.

8-72. A classic example of this is a search for TS documents stolen from the SCIF. During the search, the documents are found in the subject's office, next to a computer and scanner. While it is logical to assume that the subject is scanning the documents, such logic does not permit the CI special agent to search or seize the computer or scanner. Instead, the CI special agent must request that the scope of the authorization be expanded by submitting the request with the additional details, outlining the additional probable cause which now involves the computer and scanner, and get authorization, before the items may be seized.

What May Be Seized

8-73. There are several different types of items that may be seized during a search and seizure. These include—

- The stated evidence of the crime.
- Other contraband discovered in "plain view" within the scope of the search authorization. This can include items like drugs or weapons.
- Fruits of the crime. Property which has been wrongfully taken or possessed because of the crime. This could include the case received by the subject after the sale of the TS documents.
- Means of commission. This covers tools and other means of committing the crime, which could include lock-picks, computers, and other tools.
- Other related evidence. This focuses on more circumstantial evidence, such as clothing or other items that may place the subjects at the scene of the crime without themselves being considered to be tools.

APPREHENSION AND DETENTION AUTHORITY

8-74. CI special agents have the authority to apprehend, and a limited ability to detain, as discussed below.

Apprehension

8-75. CI special agents may apprehend individuals subject to the UCMJ anywhere in the world, on-post or off-post, when they have probable cause and reasonable belief that the Soldier committed a crime within CI jurisdiction; however, this will initiate the 120-day time line trial requirement. CI special agents should not apprehend without consulting with their SJA. If they do so, they must contact their SJA as soon as possible after the apprehension. Any delay increases the likelihood that the subject's case will be dismissed.

Detention

8-76. CI special agents may, in some circumstances, detain civilians (persons not subject to the UCMJ), and hold them long enough to turn them over to the appropriate civilian LEA. Such detention still requires probable cause and reasonable belief that the civilian committed a crime within CI jurisdiction. CI special agents may detain civilians inside the United States only on military installations. CI special agents may not detain civilians in the United States outside a military installation. Outside the United States, the CI special agent may still detain on military installations. The authority of the CI special agent to detain civilians off the installation outside the United States requires coordination and authorization by the HN as well as the required legal documentation. CI special agents should consult with the local SJA.

INVESTIGATIVE STOPS

8-77. Persons subject to the UCMJ: CI special agents may conduct an investigative stop of someone subject to the UCMJ anywhere in the world, on-post or off-post, based upon a reasonable suspicion (less than probable cause) that they committed a crime within CI jurisdiction.

8-78. Persons not subject to the UCMJ: CI special agents may conduct an investigative stop of a civilian in the United States only on the military installation. As above, such a stop requires reasonable suspicion that they committed a crime within CI jurisdiction. CI special agents may not conduct investigative stops of civilians off-post within CONUS. OCONUS, the CI special agent may conduct investigative stops on the installation. The off-post authority is again subject to SOFAs.

OATH ADMINISTRATION

8-79. Who may swear: CI special agents, both military and civilian, have the authority to swear a witness or subject to an oath. The combination of the written statement and the oath renders the statement made an "official statement," and if the witness or subject lies in such an official statement, the witness or subject may be punished for the false official statement, regardless of whether or not a conviction is obtained based upon the original allegations being investigated by Army CI.

8-80. Title and Authority: The authority to swear a witness or subject to an oath arises from Article 136(b), UCMJ (for military CI special agents) or 5 USC 303(b) (for civilian CI special agents). It is critical that CI special agents properly cite the code citation or UCMJ article and properly identify themselves; for example: "CI special agent, Army."

CRIMES AND INCIDENTS WITHIN COUNTERINTELLIGENCE INVESTIGATIVE JURISDICTION

8-81. CI special agents should bear in mind that not all crimes are solely within CI jurisdiction. In some cases, the CI special agent will be limited to investigating only CI aspects of the crime, or may be required to conduct the investigation jointly with another agency, or even with the chain of command.

CRIMES UNDER THE UNITED STATES CODE

8-82. Following is a list of crimes, including elements, within CI jurisdiction, that fall under Title 18, USC—Federal Criminal Law.

- Treason and treason-related offenses:
  - ***Treason—Levying War, 18 U.S.C § 2381. Elements:*** (1) Owing allegiance to the United States (U.S. citizen); and (2) levying war against the United States, including working with a military force raised to oppose the U.S. Government; assembling and arming a body of people for the purpose of overthrowing or opposing U.S. Government (overlaps sedition); or participating in insurrection against, or raising up a body of people to violently oppose the U.S. Government.
  - ***Treason—Aid and Comfort, 18 USC § 2381. Elements:*** (1) Owing allegiance to the United States (U.S. citizen); and (2) providing aid and comfort to our enemies, including participating in enemy propaganda; assisting a spy; committing acts of cruelty against American POWs in an enemy country; or trafficking with known enemies, in time of war, with knowledge of their hostile mission and intentionally giving aid in executing it.
  - ***Misprision of Treason, 18 USC § 2382. Elements:*** (1) Owing allegiance to the United States (U.S. citizen); (2) having knowledge of the commission of any treason against the United States; and (3) concealing and not, as soon as may be, disclosing or making known the same to the President or to some judge of the United States, or to the governor or to some judge or justice of a particular State.
- Espionage and espionage-related offenses:
  - ***Espionage, 18 USC § 794(a). Elements:*** (1) Communicating, delivering, transmitting, or attempting the same; (2) national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national defense; (3) to a foreign government, faction, agent, representative, citizen, and others (recognized or unrecognized); and (4) with the intent, or reason or reason to believe, that the information will be used to the injury of the United States or to the advantage of a foreign nation.
  - ***Espionage in Time of War, 18 USC § 794(b). Elements:*** (1) Communicating, delivering, transmitting, collecting, recording, publishing, or attempting the same; (2) in the time of

war; (3) information with respect to the movement, numbers, description, condition, or disposition of the Armed forces or war materials of the United States; and (4) with the intent that the information shall be communicated to the enemy.

- ***Entering Places Connected with National Defense, 18 USC § 793(a). Elements:*** (1) Entering, flying over, or obtaining information concerning defense installations, bases, vessels, aircraft (or any place designated off-limits by proclamation during time of war or national emergency); (2) for the purpose of obtaining information about national defense; (3) with the intent, or reason or reason to believe, that the information will be used to the injury of the United States or to the advantage of a foreign nation.
- ***Gathering Defense Information, 18 USC § 793(b). Elements:*** (1) Copying, taking, making, obtaining, or attempting the same; (2) national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national defense; (3) with the intent, or reason or reason to believe, that the information will be used to the injury of the United States or to the advantage of a foreign nation.
- ***Unlawfully Receiving Defense Information, 18 USC § 793(c). Elements:*** (1) Receiving, obtaining, or agreeing or attempting to receive or obtain; (2) from any person or source whatever; (3) national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national defense; (4) knowing, or having reason to believe, at the time received or obtain, or the time of the agreement or intent, that it has, or will be obtained, taken, made, or disposed of by any person contrary to Title 18, Chapter 37, Espionage.
- ***Transmitting National Defense Information to Unauthorized Persons, 18 USC § 793(d). Elements:*** (1) Having lawful possession of, access to, control over, or entrusted with; (2) national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national defense; (3) which the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation; (4) willfully communicates, delivers, transmits, or attempts or causes the same; and (5) to any person not entitled to receive it.
- ***Unauthorized Retention of National Defense Information by Authorized Persons, 18 USC § 793(d). Elements:*** (1) Having lawful possession of, access to, control over, or entrusted with; (2) national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national defense; (3) which the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation; and (4) willfully retaining the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it.
- ***Unauthorized Possession and Transmission of National Defense Information to Unauthorized Persons, 18 USC § 793(e). Elements:*** (1) Having unauthorized possession of, access to, or control over; (2) national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national defense; (3) which the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation; (4) willfully communicates, delivers, transmits, or attempts or causes the same; and (5) to any person not entitled to receive it.
- ***Unauthorized Retention of National Defense Information by Unauthorized Persons, 18 USC § 793(e). Elements:*** (1) Having unauthorized possession of, access to, or control over; (2) national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national

defense; (3) which the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation; and (4) willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it.

- ***Negligent Loss of National Defense Information, 18 USC § 793(f). Elements:*** (1) Having lawful possession of, control over, or entrusted with; (2) national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national defense; and (3) through gross negligence permitting the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of that trust.
- ***Failure to Report the Loss of National Defense Information, 18 USC § 793(f). Elements:*** (1) Having lawful possession of, control over, or entrusted with; (2) national defense information, including sketches, photographs, blueprints, plans, maps, models, documents, writings, or other information connected with national defense; and (3) having knowledge that the same has been lost, stolen, abstracted, destroyed, illegally removed from its proper place of custody, or delivered to anyone in violation of that trust; and (4) fails to make prompt report of such loss, theft, abstraction, destruction, illegal removal, or illegal delivery to his superior officer.
- ***Photographing and Sketching Defense Installations, 18 USC § 795. Elements:*** (1) Photographing or otherwise taking a picture of, sketching, drawing, mapping, or creating a graphical representation of; (2) military and naval installations and equipment that are vital to the interests of national defense, and therefore require protection against the general dissemination of information pertaining to them; (3) without first obtaining permission of the commanding officer of the military or naval installation or equipment, or higher authority; and (4) promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary.
- ***Use of Aircraft to Photograph Defense Installations, 18 USC § 796. Elements:*** (1) Using, or permitting the use of an aircraft or any contrivance used or designed for navigation or flight in the air; (2) for the purpose of making; (3) a photograph, sketch, picture, drawing, map, or graphical representation of; and (4) military and naval installations and equipment that are vital to the interests of national defense, and therefore require protection against the general dissemination of information pertaining to them.
- ***Publication and Sale of Photographs of Defense Installations, 18 USC § 797. Elements:*** (1) Reproducing, publishing, selling, or giving away any; (2) photograph, sketch, picture, drawing, map, or graphical representation of; (3) military and naval installations and equipment that are vital to the interests of national defense, and therefore require protection against the general dissemination of information pertaining to them; (4) without first obtaining permission of the commanding officer of the military or naval installation or equipment, or higher authority; and (5) unless such photograph, sketch, picture, drawing, map, or graphical representation has clearly indicated thereon that it has been censored by the proper military or naval authority.
- ***Disclosure of Classified Communications Information to Unauthorized Persons, 18 USC § 798. Elements:*** (1) Knowingly and willfully; (2) communicating, furnishing, transmitting, or otherwise making available to an unauthorized person; (3) any classified communications information, including information pertaining to codes, ciphers, cryptographic systems, communication intelligence systems or activities of the United States or any foreign government.
- ***Disclosure of Classified Communications Information, General, 18 USC § 798. Elements:*** (1) Knowingly and willfully; (2) publishing, or using in any manner

prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States; (3) any classified communications information, including information pertaining to codes, ciphers, cryptographic systems, communication intelligence systems or activities of the United States or any foreign government.

- Subversion and subversion-related offenses:
  - ***Subversion, 18 USC § 2387. Elements:*** (1) Advising, counseling, urging, or in any manner causing or attempting to cause insubordination, disloyalty, mutiny, or refusal of duty by any member of the U.S. military or naval forces; and (2) with intent to interfere with, impair, or influence the loyalty, morale, or discipline of the military.
  - ***Distribution of Subversive Literature to the Military, 18 USC § 2387. Elements:*** (1) Distributing or attempting to distribute; (2) any written or printed matter which advises, counsels, or urges insubordination, disloyalty, mutiny, or refusal of duty by any member of the U.S. military or naval forces; (3) with intent to interfere with, impair, or influence the loyalty, morale, or discipline of the military.
  - ***Subversion in Time of War, 18 USC § 2388. Elements:*** (1) Willfully causing or attempting to cause insubordination, disloyalty, mutiny, or refusal of duty, in the U.S. military or naval forces, or willfully obstructing the recruiting or enlistment service of the United States; (2) when the United States is at war; and (3) to the injury of the Service or the United States.
  - ***Subversive Statements in Time of War, 18 USC § 2388. Elements:*** (1) Willfully making or conveying false reports or false statements; (2) when the United States is at war; (3) with intent to interfere with the operation or success of the U.S. military or naval forces or to promote the success of its enemies.
- Sedition and sedition-related offenses:
  - ***Rebellion or Insurrection, 18 USC § 2383. Elements:*** (1) Inciting, assisting, or engaging in; and (2) any rebellion or insurrection against the U.S. authority or the laws thereof, or gives aid or comfort thereto.
  - ***Seditious Conspiracy, 18 USC § 2384. Elements:*** (1) Two or more persons in any place subject to the jurisdiction of the United States; and (2) conspiring to overthrow, put down, or to destroy by force the U.S. Government, or to levy war against them, or to oppose by force the authority thereof, or by force to prevent, hinder, or delay the execution of any U.S. law, or by force to seize, take, or possess any U.S. property contrary to the authority thereof.
  - ***Sedition, 18 USC § 2385. Elements:*** (1) Knowingly or willfully; (2) advocating, abetting, advising, or teaching the duty, necessity, desirability, or propriety of overthrowing or destroying; (3) the U.S. Government or any State, Territory, District, Possession, Country, or other political subdivisions; and (4) by force or violence, or by the assassination of any officer of any such government.
  - ***Seditious Literature, 18 USC § 2385. Element:*** (1) Printing, publishing, editing, issuing, circulating, selling, distributing, or publicly displaying any written or printed matter advocating, advising, or teaching the duty, necessity, desirability, or propriety of overthrowing or destroying (and attempts to do the same); (2) the U.S. Government or any State, Territory, District, Possession, Country, or other political subdivisions; (3) with intent to cause the overthrow or destruction of any such government.
  - ***Seditious Organizations—Organizing, 18 USC § 2385. Elements:*** (1) Organizing or helping or attempting to organize; (2) any society, group, or assembly of persons who teach, advocate, or encourage the overthrow or destruction of; (3) the U.S. Government

or any State, Territory, District, Possession, Country, or other political subdivisions; and (4) by force or violence.

- ***Seditious Organizations—Membership, 18 USC § 2385. Elements:*** (1) Being or becoming a member of, or affiliating with; (2) any society, group, or assembly of persons who teach, advocate, or encourage the overthrow or destruction of; (3) the U.S. Government or any State, Territory, District, Possession, Country, or other political subdivisions; (4) by force or violence; and (5) knowing the purposes of such society, group, or assembly or persons.

- Sabotage and sabotage-related offenses:
  - ***Sabotage—Destruction of War Material, 18 USC § 2153. Elements:*** (1) When the United States is at war, or during a time of emergency; (2) willfully damaging or destroying; (3) any war material; (4) with the intent to injure or obstruct the ability of the United States to carry out war; and (5) at the direction of a FISS and ITO or adversarial intelligence service.
  - ***Sabotage—Production of Defective War Material, 18 USC § 2154. Elements:*** (1) When the United States is at war, or during a time of emergency; (2) willfully making, constructing, or causing to be made or constructed; (3) in a defective manner (and attempts to do the same); (4) any war material; (5) with the intent to injure, interfere with, or obstruct, the ability of the United States or any associate nation, to prepare for, or carry on the war or defense activities, or with reason to believe that the act may injure, interfere with, or obstruct the United States or any associate nation in preparing for or carrying on the war or defense activities; and (6) at the direction of a FISS and ITO or adversarial intelligence service.
  - ***Sabotage—Destruction of National Defense Material, 18 USC § 2155. Elements:*** (1) Willfully damaging or destroying; (2) national defense material; (3) with the intent to injure or obstruct the U.S. national defense; and (4) at the direction of a FISS and ITO or adversarial intelligence service.
  - ***Sabotage—Production of Defective National Defense Material, 18 USC § 2156. Elements:*** (1) Willfully making, constructing, or causing to be made or constructed; (2) in a defective manner (and attempts to do the same); (3) any national defense material; (4) with the intent to injure, interfere with, or obstruct, the U.S. national defense; and (5) at the direction of a FISS and ITO or adversarial intelligence service.
- Terrorism and terrorism-related offenses:
  - Notes on Terrorism directed Against Army, 18 USC §§ 2331-2339c (chapter 113b).
  - Terrorism is any activity that involves (see 18 USC §§ 2332(b) and 2339) violent acts, acts dangerous to human life, acts that are a violation of the U.S. criminal laws or of any State, or acts that would be a criminal violation if committed within the U.S. jurisdiction or of any State; or that appear to be intended to intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; or affect the conduct of a government by mass destruction, assassination, or kidnapping.
  - Terrorist organizations are those organizations designated as terrorist organizations under section 219 of the Immigration and Nationality Act (8 USC § 1189). Releases concerning Terrorist organizations in general can be found at: http://www.state.gov/s/ct/rls/. Fact sheets on foreign terrorist organizations can be found at: http://www.state.gov/s/ct/rls/fs/. Country reports on terrorism can be found at: http://www.state.gov/s/ct/rls/crt/.
  - WMD includes an explosive, incendiary, poison gas, bomb, grenade, rocket (more than 4-oz propellant), missile (more than ¼-oz explosive or incendiary warhead), mine, similar device; any weapon designed or intended to cause death or serious bodily injury

through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; any weapon involving a biological agent, toxin, or carrier of the same; or any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. WMDs do not include chemical weapons, including toxic chemicals and their precursors, munitions, or devices specifically designed to cause death or other harm through toxic properties of those toxic chemicals, or any equipment specifically designed for use directly in connection with the employment of such munitions or devices.

- Jurisdiction requires that acts of terrorism be directed against the Army, or against Army personnel.
- ***Terrorism—Murder, 18 USC § 2332(a). Elements:*** (1) Killing a U.S. national while they are outside the United States; (2) unlawfully; (3) with malice aforethought, including using poison, lying in wait, or any other kind of willful, deliberate, malicious, or premeditated killing; or killing in the perpetration of, or attempt to perpetrate, any arson, escape, murder, kidnapping, treason, espionage, sabotage, aggravated sexual abuse or sexual abuse, child abuse, burglary, or robbery; or perpetrated as part of a pattern or practice of assault or torture against a child or children; or perpetrated from a premeditated design unlawfully and maliciously to effect the death of any human being other than the person who is killed; and (4) directed against the Army or Army personnel.
  - ***Terrorism—Voluntary Manslaughter, 18 USC § 2332(a). Elements:*** (1) Killing a U.S. national while the national is outside the United States; (2) unlawfully; (3) without malice aforethought during a sudden quarrel or in the heat of passion; and (4) directed against the Army or Army personnel.
  - ***Terrorism—Involuntary Manslaughter, 18 USC § 2332(a). Elements:*** (1) Killing a U.S. national while the national is outside the United States; (2) unlawfully; (3) without malice aforethought during the commission of an unlawful act not amounting to a felony, or in the commission in an unlawful manner, or without due caution and circumspection, of a lawful act which might produce death; and (4) directed against the Army or Army personnel.
- ***Terrorism—Attempted Murder, 18 USC § 2332(b). Elements:*** (1) Attempting to kill a U.S. national while the national is outside the United States; (2) unlawfully; (3) with malice aforethought, including using poison, lying in wait, or any other kind of willful, deliberate, malicious, or premeditated killing; or killing in the perpetration of, or attempt to perpetrate, any arson, escape, murder, kidnapping, treason, espionage, sabotage, aggravated sexual abuse or sexual abuse, child abuse, burglary, or robbery; or perpetrated as part of a pattern or practice of assault or torture against a child or children; or perpetrated from a premeditated design unlawfully and maliciously to effect the death of any human being other than the person who is killed; and (4) directed against the Army or Army personnel.
  - ***Terrorism—Conspiracy to Commit Murder, 18 USC § 2332(b). Elements:*** (1) Engaging in a conspiracy to kill a U.S. national outside the United States; (2) unlawfully; (3) with malice aforethought, including using poison, lying in wait, or any other kind of willful, deliberate, malicious, or premeditated killing; or killing in the perpetration of, or attempt to perpetrate, any arson, escape, murder, kidnapping, treason, espionage, sabotage, aggravated sexual abuse or sexual abuse, child abuse, burglary, or robbery; or perpetrated as part of a pattern or practice of assault or torture against a child or children; or perpetrated from a premeditated design unlawfully and maliciously to effect the death of any human being other than the person who is killed; (4) committing an overt act to affect the conspiracy; and (5) directed against the Army or Army personnel.
  - ***Terrorism—Other Acts, 18 USC § 2332(c). Elements:*** (1) Engaging in physical violence outside the United States; (2) with the intent to cause serious bodily injury

to a U.S. national, or with the result that serious bodily injury is caused to a national of the United States; and (3) directed against the Army or Army personnel.

- ***Terrorism—Use of WMDs Against the United States, 18 USC § 2332(a). Elements:*** (1) Using, threatening, or attempting or conspiring to use; (2) without lawful authority; (3) a WMD; (4) against a U.S. national while the national is outside the United States; against any person within the United States, where the results of such use affect, or would have affected, interstate or foreign commerce; or against any property owned, leased or used by the United States or any of its departments or agencies; and (5) directed against the Army or Army personnel.
- ***Terrorism—Use of WMDs by U.S. Nationals Outside the United States, 18 USC § 2332(b). Elements:*** (1) A U.S. national; (2) using, threatening, or attempting or conspiring to use; (3) without lawful authority; (4) a WMD; (5) outside the United States; and (6) directed against the Army or Army personnel.
- ***Terrorism—Acts Transcending National Boundaries Involving Persons, 18 USC § 2332(b)(a)(1)(A). Elements:*** (1) Engaging in conduct that transcends national boundaries, including the use of mail, or facilities of foreign or interstate commerce; (2) which involves the killing, kidnapping, or maiming of, or committing an assault resulting in serious bodily injury against, or assaulting with a deadly weapon; (3) a U.S. Government employee, including military, legislative, executive, or judicial employees, or the employee of any other U.S. department or agency; (4) within the United States, within the U.S. territorial seas, or within the special maritime or U.S. territorial jurisdiction; and (5) directed against the Army or Army personnel.
- ***Terrorism—Acts Transcending National Boundaries Involving Property, 18 USC § 2332(b)(a)(1)(A). Elements:*** (1) Engaging in conduct that transcended national boundaries, including the use of mail, or facilities of foreign or interstate commerce that; (2) creates a substantial risk of serious bodily injury to any other person by destroying or damaging; (3) any U.S. Government property, facilities, structures, or conveyances, or other real or personal property belonging to the U.S. Government; or where the offense obstructs, delays, or affects foreign or interstate commerce (including attempt or conspiracy to do the same); (4) within the United States, within the U.S. territorial seas of, or within the special maritime or U.S. territorial jurisdiction; and (5) directed against the Army or Army personnel.
- ***Terrorism—Bombing Public Place and Facilities, 18 USC § 2332(f). Elements:*** (1) Delivering, placing, discharging, or detonating an explosive or other lethal device; (2) in, into, or against, (3) a place of public use, a state or government facility, a public transportation system, or an infrastructure facility; (4) within the U.S. jurisdiction as defined by 18 USC § 2332(f); (5) with the intent to cause death or serious bodily injury, or with the intent to cause extensive destruction of such place, facility, system, or where such destruction results in, or is likely to result in major economic loss; and (6) directed against the Army or Army personnel.
- ***Terrorism—Harboring Terrorists, 18 USC § 2339. Elements:*** (1) Harboring or concealing; (2) a person who has committed, or is about to commit (or where there is reasonable grounds to believe that they have committed or are about to commit); (3) certain Federal crimes of terrorism, as defined by 18 USC §§ 2332(b) and 2339; and (4) directed against the Army or Army personnel.
- ***Terrorism—Providing Material Support to Terrorists, 18 USC § 2339A. Elements:*** (1) Providing material support or resources, including money or financial instruments, lodging, training, expert advice or assistance, safe-houses, false documentation of identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, or other physical assets other than medicine or religious materials; or concealing or disguising the nature, location, source, or ownership of material support or resources; (2) to a person or group; (3) knowing or intending that the material support or resources are to be used in

preparation for, or in carrying out; or in preparation for, or in carrying out, the concealment of an escape from the commission of (including attempts and conspiracy to do the same); (4) certain federal crimes of terrorism, as defined by 18 USC §§ 2332(b) and 2339; and (5) directed against the Army or Army personnel.

- ***Terrorism—Providing Material Support to Terrorist Organizations, 18 USC § 2339B. Elements:*** (1) Knowingly providing material support or resources, including money or financial instruments, lodging, training, expert advice or assistance, safe-houses, false documentation of identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, or other physical assets other than medicine or religious materials; or concealing or disguising the nature, location, source, or ownership of material support or resources (including attempts and conspiracy to do the same); (2) within the United States or subject to the U.S. jurisdiction; (3) to a terrorist organization, as designated by 8 USC § 1189; and (4) that directs their activities against the Army or Army personnel.
- ***Terrorism—Financing Terrorism, 18 USC § 2339C(a). Elements:*** (1) Directly or indirectly; (2) willfully and unlawfully; (3) providing or collecting funds; (4) with the intention that such funds be used, or with the knowledge that such funds are to be used, in full or in part, to carry out; (5) any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act; or where the act constitutes an offense within the scope of a treaty specific in 18 USC § 2339C(e)(7); and (6) directed against the Army or Army personnel.
- ***Terrorism—Concealing Information Pertaining to the Financing of Terrorism, 18 USC § 2339C(c). Elements:*** (1) Knowingly concealing or disguising; (2) within the United States, or subject to the U.S. laws; (3) the nature, location, source, ownership, or control of any material support, resources, or funds as defined by 18 USC § 2339B; (4) knowing or intending that the material support, resources, or funds were provided to persons engaged in terrorism or terrorist acts, to a terrorist organization, or to some person, group, or organization planning to engage in certain federal crimes of terrorism (as defined by 18 USC §§ 2332(b) and 2339); in violation of 18 USC § 2339B; or knowing or intending that such funds or any proceeds of such funds were provided or collected in violation of 18 USC § 2339C(a); and (5) directed against the Army or Army personnel.

CRIMES UNDER THE UNIFORM CODE OF MILITARY JUSTICE

8-83. Following is a list of crimes, including elements, within CI jurisdiction, that fall under the UCMJ:

- **Aiding the Enemy (Treason), Art. 104, UCMJ. Elements:** (1) Aiding the enemy; (2) with arms, ammunition, supplies, money, or other things.
- **Aiding the Enemy—Harboring or Protecting the Enemy (Treason), Art. 104, UCMJ. Elements:** (1) Harboring or protecting a person; (2) who is an enemy; (3) without proper authority; (4) knowing that the person being harbored or protected is an enemy.
- **Aiding the Enemy—Giving Intelligence to the Enemy (Treason), Art. 104, UCMJ. Elements:** (1) Knowingly giving; (2) intelligence information that is true, or implied the truth, at least in part; (3) to an enemy; (4) without proper authority.
- **Aiding the Enemy—Communicating with the Enemy, Art. 104 (Treason), UCMJ. Elements:** (1) Communicating, corresponding, or holding intercourse with; (2) an enemy; (3) knowing that the person was the enemy; (4) without proper authority.

- **Spies—Art. 106, UCMJ. Elements:** Any person who in time of war is found lurking as a spy or acting as a spy in or about any place, vessel, or aircraft, within the control or jurisdiction of any of the armed forces, or in or about any shipyard, any manufacturing or industrial plant, or any other place or institution engaged in work in aid of the prosecution of the war by the United States, or elsewhere.
- **Espionage—Art. 106a, UCMJ. Elements:** (1) Communicating (delivering, transmitting); (2) national defense information (documents, plans, blueprints); (3) to a foreign government (faction, agent, representative, citizen); (4) with the intent, or reason or reason to believe, that the information will be used to the injury of the United States or to the advantage of a foreign nation.
- **Mutiny by Violence—Art. 94, UCMJ. Elements:** (1) Creating violence or disturbance; (2) with the intent to overthrow lawful military authority.
- **Mutiny by Refusal—Art. 94, UCMJ. Elements:** (1) Refusing to obey orders; (2) in concert with another; (3) with the intent to overthrow lawful military authority.
- **Sedition—Art. 94, UCMJ. Elements:** (1) Creating a revolt, violence, or disturbance; (2) against lawful civil authority; (3) in concert with another; (4) with the intent to overthrow or destroy that authority.
- **Failure to Prevent and Suppress Mutiny or Sedition—Art. 94, UCMJ. Elements:** (1) Witnessing an offense of mutiny or sedition; (2) failing to do your utmost to prevent and suppress the mutiny or sedition.
- **Failure to Report Mutiny or Sedition—Art. 94, UCMJ. Elements:** (1) Knowing, or having reason to know; (2) that an offense of mutiny or sedition was taking place; (3) failing to take all reasonable means to inform your superior commission officer or commander of the offense.
- **Attempted Mutiny,—Art. 94, UCMJ. Elements:** (1) Committing a certain overt act; (2) with the specific intent to commit mutiny; (3) where the act amounted to more than mere preparation; and (4) where the act apparently tended to effect the commission of the mutiny.
- **Destruction of Military Property—Art. 108, UCMJ. Elements:** (1) Intentionally; (2) without authority; (3) damaging or destroying; (4) U.S. military property; (5) of a certain value; (6) at the direction of a FISS and ITO or adversarial intelligence service.
- **Defection—Modeled from Desertion—Art. 85, UCMJ). Elements:** (1) Leaving your unit or place of duty; (2) departing the United States or country in which you are stationed; and (3) Repudiating (rejecting or disowning) the United States and U.S. authority.
- **Desertion with Intent to Remain Away Permanently—Art. 85, UCMJ. Elements:** (1) Leaving your unit or place of duty; (2) without authority; (3) intending to remain away permanently; (4) having had access within the last year to TS information, SCI, SAPs, DA Cryptographic Access Program (DACAP), or were part of a Special Mission Unit; and (5) if they are apprehended, remaining away until the date alleged.
- **Absence Without Leave—Art. 86, UCMJ. (Use this as model for personnel who are missing.) Elements:** (1) Absenting yourself from your unit or place of duty; (2) without authority; (3) for a certain period of time; (4) having had access within the last year to TS information, SCI, SAPs, DACAP, or were part of a special mission unit.

- **Security Violation—Information Security, Violation of a Regulation, Art. 92, UCMJ. Elements:** (1) A regulation (AR 380-5) was in effect; (2) the accused had a duty to obey that regulation; (3) the accused failed to obey that regulation, including (a) failing to safeguard classified information; (b) the loss or possible compromise of classified information; (c) unauthorized reproduction of classified information; or (d) failure to properly wrap classified materials.
- Security Violation—Failure to Report CI Incident, Violation of a Regulation, Art. 92, UCMJ. Elements: (1) A regulation (AR 381-12) was in effect; (2) the accused had a duty to obey that regulation; (3) the accused failed to obey that regulation.

OTHER INCIDENTS UNDER COUNTERINTELLIGENCE JURISDICTION

8-84. Following is a list of other incidents under counterintelligence jurisdiction (CIJ).

- Assassination of Army personnel by nonterrorist organization or individuals:
  - Committed by military personnel. Use Murder, Art. 118, UCMJ.
  - Committed by nonmilitary U.S. person under CIJ. Use Murder, 18 USC § 1111.
  - Committed by nonmilitary non-U.S. person under CIJ. Use Murder, 18 USC § 1111 as a guide.
  - ***Committed by person outside CIJ.*** Use Murder, 18 USC § 1111 as guide.
- Assassination of Army personnel by terrorist organization or individuals:
  - ***Committed by military personnel.*** Use Murder, Art. 118, UCMJ and Terrorism—Murder, 18 USC § 2332(a); look to other offenses under 18 USC § 2332 and 18 USC § 2339.
  - ***Committed by nonmilitary U.S. person under CIJ.*** Use Terrorism—Murder, 18 USC § 2332(a); look to other offenses under 18 USC § 2332 and 18 USC § 2339.
  - ***Committed by nonmilitary non-U.S. person under CIJ.*** Use Terrorism—Murder, 18 USC § 2332(a) as a guide; look to other offenses under 18 USC § 2332 and 18 USC § 2339.
  - ***Committed by person outside CIJ.*** Use Terrorism—Murder, 18 USC § 2332(a) as a guide; look to other offenses under 18 USC § 2332 and 18 USC § 2339.
- Incapacitation of Army personnel by nonterrorist organization or individuals:
  - ***Committed by military personnel.*** Use Kidnapping, Art. 134, UCMJ; Assault or Assault and Battery, Art. 128, UCMJ.
  - ***Committed by nonmilitary U.S. person under CIJ.*** Use Kidnapping, 18 USC § 1201; Assault, 18 USC §§ 111 and 113.
  - ***Committed by nonmilitary non-U.S. person under CIJ.*** Use Kidnapping, 18 USC § 1201; Assault, 18 USC §§ 111 and 113 as guides.
  - ***Committed by person outside CIJ.*** Use Kidnapping, 18 USC § 1201, Assault, 18 USC §§ 111 and 113 as guides.
- Incapacitation of Army personnel by terrorist organization or individuals:
  - ***Committed by military personnel.*** Use Kidnapping, Art. 134, UCMJ; Assault or Assault and Battery, Art. 128, UCMJ; Terrorism—Other Acts, 18 USC § 2332(c); look to other offenses under 18 USC §§ 2332 and 2339.
  - ***Committed by nonmilitary U.S. person under CIJ.*** Use Terrorism—Other Acts, 18 USC § 2332(c); look to other offenses under 18 USC §§ 2332 and 2339.

- ***Committed by nonmilitary non-U.S. person under CIJ.*** Use Terrorism—Other Acts, 18 USC § 2332(c) as a guide; look to other offenses under 18 USC §§ 2332 and 2339.
- ***Committed by person outside CIJ.*** Use Terrorism—Other Acts, 18 USC § 2332(c) as a guide; look to other offenses under 18 USC §§ 2332 and 2339.

- **Detention of DA Personnel by a Foreign Government or Hostile Force (with interests inimical to the United States). Key points:** (1) An Army Soldier, Army Civilian employee, a DA contractor, or a foreign national employed by the Army; (2) is being held against his will; (3) by a foreign government, faction, agent, representative, citizen (recognized or unrecognized); or member of a hostile force, including a terrorist, terrorist group, or terrorist organization; (4) with interest inimical to those of the United States; and (5) for any length of time.
- **Suicide of DA Personnel. Key points:** (1) An Army Soldier, Army Civilian, a contractor with DA, or a foreign national employed by the Army; (2) holding a security clearance, Secret or higher; including those with access to SCI, SAPs, who were in the DACAP, or were part of a special mission unit; and (3) who killed himself.
- **Attempted Suicide of DA Personnel. Key points:** (1) An Army Soldier, Army Civilian employee, a contractor with DA, or a foreign national employed by the Army; (2) holding a security clearance, Secret or higher; including those with access to SCI, SAPs who were in the DACAP, or were part of a special mission unit; and (3) who attempts to kill himself.
- **Unofficial Travel by Military Members (and Civilians overseas) to Designated Countries. Key points:** (1) An Army Soldier; and overseas, an Army Civilian employee, a contractor with DA, or a foreign national employed by the Army; (2) traveling to a country designated as being of special concern (AR 381-12, appendix B, contains a list, based on DCID 1/20 (Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information [SCI]); and (3) without prior notification or permission.
- **Unauthorized Contact by Military Members (and Civilians overseas) with Foreign Diplomatic Facilities. Key points:** (1) An Army Soldier; and overseas, an Army Civilian, a contractor with DA, or a or a foreign national employed by the Army; (2) entering, communicating with, or otherwise having contact with; (3) a foreign diplomatic facility, including an embassy, consulate, trade office, or press office; (4) without prior notification or permission.
- **Unauthorized Contact by Military Members (and Civilians overseas) with Foreign Diplomatic Officials or Official Representatives. Key points:** (1) An Army Soldier; and overseas, an Army Civilian employee, a contractor with the DA, or a foreign national employed by the Army; (2) communicating with or having contact with; (3) officials representing designated countries of special concern; (AR 381-12 focuses on this narrower concern, not just contact in general—use list in AR 381-12, appendix B, including diplomatic representatives, agents, and other employees of the foreign government); and (4) without prior notification or permission.
- **Inchoate crimes.** Inchoate crimes are not crimes in and of themselves. Instead, they are a unique body of law that encompasses those acts that go beyond mere planning and tend towards the commission of a crime. Depending on the acts of the accused, they may be able to be convicted of the inchoate crime as if they had, in fact, committed the crime they were planning to commit. Inchoate crimes include attempt, conspiracy, and solicitation.

Note. For Army CI purposes, this FM only addresses inchoate crimes under the UCMJ.

- Attempt—Art. 80, UCMJ:
  - Attempt occurs when the accused tries to commit a crime, but for reasons beyond their control, fails. Use the attempted crime as a guide for what acts tend to support the commission of the crime.
  - ***Elements:*** (1) Committing a certain overt act; (2) where the act is done with the specific intent to commit a crime under the code; (3) that the act amounts to more than mere preparation; and (4) that the act apparently tends to effect the commission of the crime.

Note. An example of attempted espionage would be if the subject obtained the password for JWICS without proper clearance, made contact with a foreign country as a potential buyer, and arranged the transmission method. If the subject is caught and stopped before actually transmitting the data, the Army may still be able to convict him of attempted espionage, or at least attempting one of the espionage-related offenses, such as unlawfully transmitting national defense information.

- Conspiracy, Art. 81, UCMJ:
  - Conspiracy occurs when the accused enters into an agreement with someone else to commit a crime. Use the conspired crime as a guide for what acts tend to support the commission of the crime.
  - ***Elements:*** (1) Entering into an agreement; (2) with one or more persons; (3) to commit an offense under the code; and (4) while the agreement continued to exist, and while the accused was still a party to the agreement, the accused or one of the co-conspirators; (5) committed a certain overt act; and (6) for the purpose of bringing about the object of the conspiracy.

Note. An example of a conspiracy to commit terrorism would be a Soldier stationed in Germany who makes contact with the local national guard who provides guard services at the Army and Air Force Exchange Service, then secures material to create an IED. If the Soldier is stopped before actually planting the IED, the Army may still be able to convict him of conspiracy to commit a terrorist act, such as use of a WMD, or bombing of a public place.

- Solicitation, Art. 82, UCMJ:
  - Solicitation under article 82 occurs when the accused solicits or advises another to desert (Art. 85), commit mutiny (Art. 94), misbehave before the enemy (Art. 99), or commit sedition (Art. 94). Use the conspired crime as a guide for what acts tend to support the commission of the crime. Solicitation of other crimes falls under UCMJ, article 134, and is addressed below.
  - ***Elements:*** (1) Soliciting or advising a person to commit desertion, mutiny, misbehavior before the enemy, or sedition; (2) with the intent that the offense be committed; and (3) if the offense solicited was committed or attempted, that the offense was committed or attempted as the proximate result of the solicitation.

Note. An example of solicitation under Article 82 would be a platoon sergeant who actively encourages his Soldiers to revolt against their company commander. Even if the Soldiers do not, in fact, commit mutiny, the platoon sergeant could still be found guilty of solicitation in violation of article 82.

- Soliciting Another to Commit an Offense, Art. 134, UCMJ:
  - Use article 134 for any offense not covered by solicitation under article 82. Use the conspired crime as a guide for what acts tend to support the commission of the crime.
  - ***Elements:*** (1) Soliciting or advising a person to commit a crime under the code, other than desertion, mutiny, misbehavior before the enemy, or sedition; (2) with the intent that the offense be committed; and (3) that, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces, or was of a nature to bring discredit upon the armed forces.

Note. An example of solicitation under article 134 would be a Service-member spouse stationed in Korea who does not have access to classified information, and who requests that his spouse (who does have access) copy SECRET documents for him, so that he could sell them to the South Korean government. Even if the documents are never copied or sold, the Service-member spouse without access could still be found guilty of solicitation under article 134.

Chapter 9

Counterintelligence Reporting

CI reporting is generally the culmination of the successful execution of the various types of CI activities. CI reporting is a critical input to the all-source intelligence picture and can corroborate other discipline reporting as well as tip and cue other assets collection activities. Finalized CI reports provide the commander a tangible product that impacts the MDMP and helps to shape military operations. However, CI reporting also documents evolving CI operations and investigations and allows operational management elements to conduct technical control and oversight of ongoing CI activities.

TENETS OF REPORTING

9-1. Articulation of information obtained during the course of CI activities is a skill that takes time, repetition, and mentorship to master. CI reports not only have to reflect the information obtained during the course of CI activities but also must often anticipate the analyst or commander's questions concerning lack of detail or information gaps that must be addressed to help further shape the ISR collection effort. The tenets of reporting include the following:

- **Accuracy.** Convey information from an interview or meeting and transcribe it into a protected operational or intelligence report. The report writer should never infer or otherwise interpret a source's meaning or understanding of the information provided to the CI special agent.
- **Conciseness.** Cover only the facts or information provided by the source. Analysts and commanders have volumes of information to synthesize to form their operational assessments. Reports should not be wordy. The information conveyed should be to the point while providing the full depth of the information.
- **Clarity.** Convey the information in simple wording as possible. Writers should use short sentences and logically arrange the information so as not to confuse the reader.
- **Timeliness.** Disseminate the information through the appropriate reporting channel in the most expedient manner as possible. While written reports are preferable, the perishability and sensitivity of the information may dictate that the information requires reporting via voice communications with a follow-up written report.
- **Admissibility.** Use standardized formats and legal warnings and verbiage to maintain a prosecutorial standard in the event the reports are used during criminal proceedings. CI investigative reports can serve as the CI special agent's testimony during criminal proceedings if that person is unavailable. Poorly written, unclear, or confusing investigative reports can be exploited by defense counsels to portray the reporting CI special agent as inept in an attempt to confuse or sway a judge or jury in favor of the defendant.

REPORTS MANAGEMENT

9-2. Reports management is the process for ensuring a quality report product, evaluating the information for its relevance and value to the consumer and its impact on generating new or derivative information requirements based upon the reported information. The quality and value of report products are critical in maintaining trust and credibility with the consumers who use those products to drive military operations or shape U.S. policies and objectives. Reports management entails the following roles and functions.

REPORTS OFFICER

9-3. The importance of reports management is often reflected in units with a large reporting mission by the designation of a reports officer, whose responsibilities include—

- Providing administrative and information quality control (QC) for all reports generated by CI teams.
- Assessing information by multiple reporting elements to deconflict information, assess the value of reporting, and help shape the collection focus provided by operational management elements.
- Coordinating with analysis elements to identify what requirements are being answered, requirements that need additional emphasis, and assist in the development of new information requirements based upon credible and corroborated reporting.
- Disseminating evaluations to reporting elements to assist them in adjusting their operational focus and to provide feedback on the quality and value of their previous reporting.
- Maintaining reporting statistics to assist operational management elements in refining their technical authority and operational guidance to subordinate reporting elements.
- Assisting operational management elements in assessing source placement, access, value, and credibility based upon historical reporting. This allows the operational management elements to make decisions on directing source terminations for subordinate reporting elements.

QUALITY CONTROL

9-4. QC is the oversight of reports production to ensure a quality product is disseminated from the reporting element to the consumers who use the information. QC ensures that the tenets of reporting are adhered to by the writers. QC includes the following:

- Administrative QC—ensures writers adhere to applicable regulatory guidance and unit SOPs for format, verbiage, and other administrative criteria that are required in the reports.
- Information QC—analyzes the information content to identify inconsistencies within the report or conflicts with other credible and corroborated reporting.

REPORT EVALUATIONS

9-5. Report evaluations are essential in assessing the quality and value of the report as it relates to the consumer of the information. Reports evaluations are used by operational management elements to adjust or refine the collection focus for CI reporting elements.

REQUIREMENTS GENERATION

9-6. CI reporting and reports management also impacts the requirements generation process. Requirements may be added, deleted, or revised based upon information assessed as credible and corroborated by other reporting.

REPORT CATEGORIES

9-7. CI elements produce several different types of reports to support their mission. These different reporting requirements fall into three categories:

- **Command reports**—include unit status reports (USRs) and all reporting requirements established by a commander (logistical, equipment, personnel) to reflect the unit's readiness to execute its assigned mission. Command reports—
  - Tell the commander where and when assets are conducting missions.

- Describe unit mission capability.
- Respond to administrative and logistical requirements.
- Describe support requirements.
- Include but are not limited to USRs, mission planning reports, mission status reports, and equipment status.
- Report ICF usage at any echelon where the use of ICF is authorized.

- **Protected reports**—include the various types of CI reports that result from an operational activity. Protected reports require compartmentalization within the CI operations management chain (CI team, OMT, CICA, 2X) to protect the identity and details of CI activities. Due to the sensitivity and legal complexities associated with CI activities, only the technical authorities for CI activities will have access to the information. This protects the CI special agent and the source. If a CI activity is compromised due to an information leak, it has the potential to compromise the viability of the activity; be harmful, if not fatal, to a CI special agent and especially the source; or undermine the legal and prosecutorial standard of CI investigations. Protected reports will NOT be released outside 2X channels without authorization of the responsible 2X officer. This includes commanders of units with CI personnel assigned or attached. Protected reports include, but are not limited to—
  - ***BSD reports***—provide the CI operational management element with biographic and operational information related to a source. BSDs are used at all echelons to collect biographic information on all contacts.
  - ***Contact reports***—CI special agents use contact reports to inform their technical authority (from OMT through C/J/G/S-2X) of all relevant information concerning specific meetings with sources. Information typically includes the circumstances of the contact (purpose, locations, time); the operational matters relative to the contact (topics discussed, taskings given); reports produced because of the contact; and logistics expended.
  - ***Lead development report***—used to inform the HUMINT chain of ongoing operations directed toward a specific source. LDRs notify them as to what element spotted the potential source, the current steps in assessing of the source, and the general information on the potential source.
  - ***Investigative reports***—include IMFRs and CI incident reports used to report any incident or national security crime within the authority and jurisdiction of Army CI. For CI investigations the protected reporting channels include the CI team, CI OMT, TFCICA (for CI elements operating within a JTF), the ATCICA, and the ACICA to provide technical authority for all CI investigations conducted by Army CI elements.
  - ***Communications plans***—developed for source-to-agent and agent-to-source contact.
  - ***Source registries***—consolidated lists of all sources used by CI teams under the technical authority of a CICA/2X. Source registries generally include identifying data, location, and associations with the CI team that if compromised could significantly damage the intelligence capability of the supported unit.
  - ***Miscellaneous***—any type of documentation that provides details on the identity of a source; methods of communication; operational activity; or meeting dates, times, or locations.
- **Intelligence reports**—include the various types of reports that are produced to disseminate for intelligence and information purposes. Intelligence reports are disseminated within intelligence channels for consumers, analysts, and commanders to use to obtain situational understanding of their respective AOIs. Intelligence reports will always be disseminated

within the intelligence reporting channels and protected channels simultaneously. This allows the operational management elements to maintain visibility over the production of the CI teams and know all sensitive or inflammatory information this is developed during the course of CI activities. Intelligence reports include, but are not limited to—

- ***IIRs***—used to report all CI information in response to collection requirements. It is used to expand on information previously reported by spot reports or to report information that is either too extensive or not critical enough for spot reporting. IIRs are written at any echelon and "released" by the appropriate authority before they enter the general intelligence community. Normally the G-2X will be the releasing authority for IIRs.
- At the tactical level, the CI special agents will fill out the complete IIR; however, the requirements section may link the information collected against a unit requirement rather than against national requirements. In any case, the report will be forwarded to the OMT.
- The team leader will review the IIR, place a copy of the IIR in the source's dossier and forward the IIR to the OMT. The OMT reviews the report, requests additional information as necessary from the originator, adds additional administrative detail, and forwards the report to the CICA of the supporting C/J/G/S-2X. The CICA and the 2X review the report, request additional information as required, add any administrative information, and the 2X releases the report.
- In addition to the above, the text information from the IIR can be forwarded to the unit's analytical elements and when it contains critical time-sensitive information, such as an impending attack, it is sent to units which may be affected by the information; however, it must be clearly marked "unevaluated information, **not** finally evaluated intelligence."
- ***Spot reports, using the SALUTE format***—standard Army format used to report information of immediate interest by individuals at any echelon. They are used to report time-sensitive information that includes protection and threat I&W to the chain of command. The spot report is the primary means used to report combat information to units that could be affected by that information. After review by the team leader, spot reports are sent simultaneously to the supported unit S-2, to the CI team's responsible CI OMT, and to the intelligence staff officer of any other tactical unit that may be affected by the information contained in the spot report. While unit SOPs may provide written formats, spot reports should be reported by the most expeditious means possible, usually voice and a follow-up written report. Spot reports are reported simultaneously to the command protected and intelligence reporting channels.
- Any type of format used to disseminate information of intelligence value or that may be used for protection, threat I&W.

REPORTING ARCHITECTURE

9-8. Many elements serve multiple and overlapping functions within the reporting architecture. Each element must know its function within the architecture to ensure that information is disseminated expeditiously to the right place in the right format. This architecture should be established and published before implementation to avoid confusion. Figure 9-1 shows this reporting architecture of the command reporting channel, protected reporting channel, and the intelligence reporting channel.

9-9. The command reporting channel includes the CI team, the responsible CI OMT, and the unit command element the CI team and OMT are assigned or formally attached to on orders. All command reporting concerning personnel, sustainment, equipment, resources, or unit readiness will be reported from the CI team to the OMT, then from the OMT to the command element. In situations where the CI team is located at a subordinate echelon from the OMT, command reports may be required to be submitted simultaneously from the CI team to the OMT and the command element. The OMT, CICA/2X is responsible for coordinating command reporting requirements.

9-10. The protected reporting channel includes the CI team, the responsible CI OMT, the CICA, and the 2X. All protected reporting concerning information that provides details on the identity of a source, methods of communication, operational activity or meeting dates, times, and locations will be reported from the CI team to the OMT, then from the OMT to the CICA, then the CICA to the 2X. The protected reporting channel is used to protect the details of CI activities and the identities of CI sources. CI teams and OMTs are not authorized to disclose details of or release information concerning any information reported within the protected reporting channel unless approved by the responsible CICA and 2X.

9-11. The intelligence reporting channel includes the CI team, the responsible CI OMT and the 2X element of the support unit. All intelligence reporting concerning information of intelligence value or that may be used for protection or threat I&W will be reported from the CI team to the OMT, then from the OMT to the intelligence staff, C/J/G/S-2. Although the intelligence staff, C/J/G/S-2 is the primary consumer of intelligence reports, all intelligence reporting from CI teams will always be disseminated within the intelligence reporting channels and protected channels simultaneously. This allows the operational management elements to exercise technical authority over CI teams under their purview and prevent the CICA and 2X from being caught off guard by sensitive or inflammatory CI reporting.

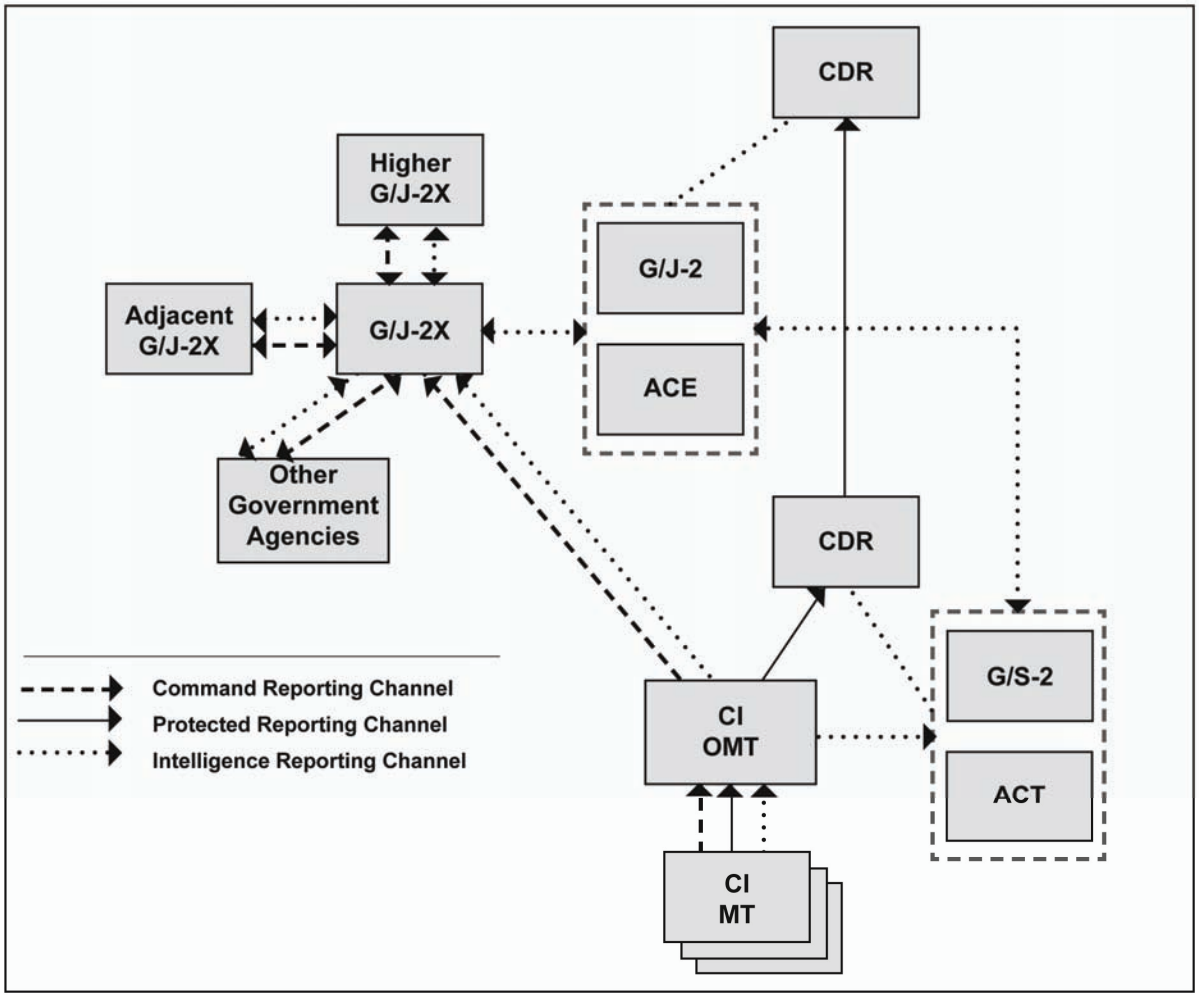

Figure 9-1. Reporting architecture

INFORMATION SHARING AND RELEASE

9-12. Units must develop SOPs for the passing of information and intelligence to multinational units. Units will coordinate with Foreign Disclosure Officers, appropriate classification authorities, and higher headquarters to develop procedures and standards to release reports and information to HN, allied, or coalition elements. Report writers and editors must ensure that reports that are to be shared with multinational units contain only releasable information. This will enable reports to have the widest dissemination. Arrangements are made through the C/J-2X/LNO for distribution. When possible, reports to be shared with multinational units should be kept to the appropriate classification to ensure the widest dissemination of the reported information.

Appendix A

Counterintelligence Program Administration

The Army Counterintelligence (CI) Program requires its members to be mature, intelligent, and personable to carry out the broad range of CI functions to detect, identify, exploit, and neutralize the foreign intelligence and security systems (FISS) and international terrorist organizations (ITO) threat targeting U.S. forces. The CI special agent has to be able to operate independently and be relied upon to make sound judgments in the absence of higher leadership or supervision. The CI special agent also has to interact with senior officials of both U.S. and host-nation (HN) military, civilian law enforcement, intelligence, and security agencies. This requires that personnel applying for the Army CI Program be among the most professional and competent Soldiers in the Army. The CI applicant process is extremely important in ensuring that the CI military occupational specialty (MOS) remains capable, and that the most qualified and competent personnel are accepted into the Army CI Program. CI special agents will conduct all interviews and processing of Army CI Program applicants.

COUNTERINTELLIGENCE APPLICANT PROCESS

A-1. The CI applicant process should never be viewed as something to be done only if a CI special agent or CI element has time for. Also, it should not be a task handed only to the most inexperienced CI special agents in a unit. While it is good training to build organizational, planning, and interpersonal skills, the CI applicant process should be about showcasing our most talented CI special agents to the CI applicant. The professionalism, maturity, confidence, and competence of the interviewing special agent, may be instrumental in assisting potential applicants in solidifying their decision to apply for the Army CI Program.

A-2. CI special agents processing CI applicants will ensure they do not form any positive or negative biases towards a potential CI applicant. All Soldiers who meet the eligibility requirements to be a CI special agent should be afforded the opportunity to apply for the CI Program. Failure to meet requirements or lack of character traits that would preclude them from being a professional and competent CI special agent will be developed during the course of the CI applicant process.

A-3. The initial interview is the first contact between the prospective CI applicant and the CI special agent. During the initial interview the CI special agent needs to explain the mission of Army CI, the eligibility requirements for becoming a CI special agent, the process that must be completed to be accepted into the Army CI Program, the training and potential assignments.

A-4. CI applicant qualifications include the following:

- A physical demands rating of Medium.
- A physical profile of 222221**.**
- Normal color vision.
- A minimum score of 102 in aptitude area ST/Technical score on the Armed Services Vocational Aptitude Battery (ASVAB).
- A minimum age of 21 years of age for award of MOS 35L accreditation as a CI special agent.

- A security clearance of interim top secret (TS) with eligibility for access to sensitive compartmented information (SCI) once TS clearance is granted.
- A high school graduate or equivalent.
- Possess good voice quality and be able to speak English without an objectionable accent or impediment.
- Never been a member of the U.S. Peace Corps.
- No derogatory information in provost marshal, intelligence, military personal records jacket (MPRJ), or medical records that would prevent the granting of a security clearance in accordance with AR 380-67.
- No records of conviction by court-martial.
- No records of conviction by civil court for any offense other than minor traffic violations.
- A U.S. citizen by birth.
    - Members of immediate family (spouse, parents, brothers, sisters, and children) must also be U.S. citizens. Soldier and immediate family members can be naturalized citizens. If naturalized, there is no minimum residency requirement.
    - Soldier and spouse must not have immediate family members who reside in a country where physical or mental coercion is known to be a common practice, against persons accused of or acting in the interest of the United States; the relatives of such persons to whom they may reasonably be considered to be bound by ties of affection, kinship, or obligation. Near relatives will also include uncles, aunts, grandparents, father-in-law, mother-in-law, and relationships corresponding to any of the above persons in *loco parentis* (AR 630-5 and 37 USC § 501).
- Have neither commercial nor vested interest in a country where physical or mental coercion is known to be a common practice against persons acting in the interest of the United States. This requirement applies to the Soldier's spouse as well.
- Have an active Army Knowledge Online (AKO) email account. If you do not have an AKO email account when your packet is sent forward, your packet will not be processed.
- To qualify under the bonus extension and retention (BEAR) program (if applicable) the Soldier must have less than 10 years of service at time of reenlistment on the day of graduation from school.

A-5. **CI applicant process.** The entire CI applicant process can be lengthy endeavor. The amount of time it takes from initial inquiry to approval and orders production will be significantly affected by the motivation of the CI applicant to get the required documentation and complete all applicant interviews and compositions.

A-6. **Initial contact and interview.** The first contact with a prospective CI applicant may be over the telephone. The CI special agent taking the call from a prospective applicant should arrange for a face-to-face meeting between the applicant and the CI special agent who will be processing the applicant. During the initial interview, the applicant should be informed of the minimum qualifications for the Army CI Program, as well as all the required documentation and the process for applying to the Army CI Program. The processing CI special agent should refrain from forming any positive or negative biases against any applicant during the process and especially the first interview. During the initial interview, if the prospective applicant is serious about pursuing the CI application process, have the applicant complete an applicant information sheet.

A-7. **CI applicant requirements.** The entire process for applying to the Army CI Program should be covered in detail in the first interview including all the required documentation the applicant will be responsible for completing or coordinating for himself. The actions that must be completed by the CI

applicant are broken down into an 11-step process. The CI applicant process is outlined in DA Pam 600-8, procedure 3-33-1, dated 1 August 1986. A copy of the DA pamphlet can typically be found at personnel and administration center (PAC) or the servicing personnel servicing company.

- Step 1:
  - ***Action required by:*** Individual.
  - ***Description of actions:*** Inform immediate supervisor and unit commander of intention to volunteer for MI service. Currently not required, but is recommended for the future MI applicant to take the Defense Language Aptitude Battery (DLAB) test at the education center.
- Step 2:
  - ***Action required by:*** Unit commander/1SG/battalion PAC/personnel services noncommissioned officer (PSNCO).
  - ***Description of actions:*** Assist Soldier in preparing DA Form 4187 (Personnel Action) requesting MI training. Privacy Act Statement will be furnished to Soldier before having individual complete DA Form 4187. (This is done by the PAC.)
- Step 3:
  - ***Action required by:*** PSNCO.
  - ***Description of actions:*** Arrange an appointment with the S-2/G-2 or security manager for completion of SF 86 (Questionnaire for National Security Positions).
  - Arrange an appointment with the photographic facility. The photograph is to be full length in class "A" uniform (or their equivalent). No civilian clothing photograph is required.
- Step 4:
  - ***Action required by:*** S-2/G-2/security manager.
  - ***Description of actions:*** Advise all applicants they must undergo a single-scope background investigation (SSBI). CI applicant must arrange with their S-2/G-2 or unit security manager to complete the SF 86. The CI applicant must include two SFs 86 in their packet. One SF 86 will be an original front and back and the second SF 86 a reproduced copy.
  - Complete two copies of FD-258 (FBI Fingerprint Card). Ensure all personal history and physical characteristics blocks are completed and both individual and person taking fingerprints sign the appropriate signature blocks.
- Step 5:
  - ***Action required by:*** Photographic facility.
  - ***Description of actions:*** Prepare 3/4-length photograph of individual in class "A" uniform (or equivalent).
- Step 6:
  - ***Action required by:*** PSNCO.
  - ***Description of actions:*** Upon completion of steps 4 and 5, arrange an appointment with military personnel office (MILPO). Have Soldier hand carry DA Form 4187 with supporting documents to the MILPO.

- Step 7:
  - ***Action required by:*** Personnel management specialist.
  - ***Description of actions:*** Obtain a MPRJ from records branch; verify that Soldier meets eligibility criteria and prerequisites contained in AR 614-200, section II, chapter 7; DA Pam 351-4; and the MOS requirements in AR 611-201. Ensure that SF 86, FD-258, and photograph are attached; prepare forwarding comment to local supporting CI element. Reproduce and attach one copy of the Soldier's DA Forms 2 and 2-1 (Personnel Qualification Record) or enlisted records brief (ERB) to the request.
- Step 8:
  - ***Action required by:*** Personnel management supervisor.
  - ***Description of actions:*** Review documents from steps 1 through 7 to ensure tasks are completed.
- Step 9:
  - ***Action required by:*** Personnel management officer.
  - ***Description of actions:*** Review and sign documents as required in steps 1 through 8.
- Step 10:
  - ***Action required by:*** Records specialist.
  - ***Description of actions:*** File copy of request for MI training as action pending document in MPRJ.
- Step 11:
  - ***Action required by:*** Personnel management specialist.
  - ***Description of actions:*** Arrange for an interview by an experienced CI special agent. On day of interview, have Soldier obtain MPRJ for review by CI special agent. Have Soldier take DA Form 4187 with enclosures to interview.

A-8. **Required documentation.** Required documentation in the CI applicant packet includes the following:

- **SF 86.** This personnel security questionnaire (SSBI) is required of all applicants, regardless of current security clearance status. In addition, a NAC on applicant's spouse is required. This is done through the S-2. The applicant must have signed copies of the back pages of the questionnaire.
- **FD-258.** FBI fingerprint card.
- **DA photograph.** One DA photograph in class A uniform is all that is required. It need not be full-length, and no civilian photograph is necessary.
- **DA Form 4187 (DA Pam 600-8, procedure 3-33-1).** It is important that the applicant have the DA Form 4187 signed by the appropriate commander, and then turned into the interviewing agent. The DA Form 4187 must accompany the rest of the packet. The THRU and FROM sections of the DA Form 4187 will be completed as norm, but will be addressed: TO: "Commander, HRC, ATTN: AHRC-EPB-M, 2461 Eisenhower Avenue, Alexandria, VA 22331-0400." In section III, part 8, the applicant must check the OTHER block and insert "MI Application, in accordance with procedure 3-33." Section IV – Remarks will contain applicant "(Rank, LAST NAME) meets all perquisites specified to reclass to MOS 35L." If the BEAR program is in effect, another line should be added: "(Rank, LAST NAME) requests retraining on BEAR program option of CI (35L) in the MI branch." In section V, ensure

applicant's commander checks the block "Recommend Approval" only. DA will check the block for "Is Approved" or "Is Disapproved."

- **Enlisted records brief.** If any additional information, pertinent to the applicant's qualifications for MOS 35L, is not recorded in the ERB, include that documentation. For instance, if a Soldier's recorded service test (ST) score on the DA Form 2-1 is no longer current, include a copy of the test results showing the updated ST score.
- **Privacy Act Advisement.** This form will be signed and dated by the applicant at the local MI office when you come in for the interview.
- **Defense Language Aptitude Battery test results (optional, but recommended).** Memorandum from tester at the education center stating the results of the test.
- **Other documents.** Any request for waivers of qualifications and explanations of events that might reflect negatively on the Soldier's suitability for the MOS 35L.
- **AKO email address.** It is now required to have an active AKO email account to process for MOS 35L. If you do not have an AKO account when your packet is sent forward, your packet will NOT be processed.

A-9. **Processing interview.** The processing interview is the next major step for a CI applicant to join the Army CI Program. Due to the significant amount of personal time and actions required for the CI Applicant process, normally only the most serious applicants will get to this point. The processing interview is the point in which the interviewing agent will collect all the required documentation required from the CI applicant.

A-10. During the processing interview, the CI applicant should be afforded the opportunity to withdraw from the application process. This allows the agent to determine the motivation and fortitude of the applicant about joining the CI Program. During the processing interview the interviewing agent will have the CI applicant complete three written exercises. These statements are designed to judge the maturity, expectations, and written skills of the CI applicant to ensure they have the character traits to complete CI training and to successfully carry out the duties and responsibilities of a CI special agent.

- **Contingency statement.** The applicant will complete the statement in his own handwriting, sign and date, in pen.
- **Motivational composition.** The applicant will be given a 10-minute time limit to complete the motivational composition in pencil stating why he is applying for the position of a CI special agent.
- **Biographical composition.** The applicant will be given a 45-minute time limit to complete the biographical composition describing their family background and other influences in their life; major fields in which they have been employed (for example, sales, office work, farming, laborer); significant incidents in their life which has affected their personality, character, or outlook on life; major interests in life and what has been done to develop them.

A-11. **Final interview.** The final interview is a final information gathering and assessment meeting between the interviewing agent and the CI applicant. Before the final interview, the interviewing agent will review all the documentation, security questionnaires, and compositions completed by the CI applicant to help the interviewing agent explore any gaps in the applicant's background or potential vulnerability and weaknesses that would indicate the applicant may be a liability as a CI special agent. During this interview the interviewing agent will also try to identify those attributes and character traits of the applicant that would make him an asset in the Army CI Program. As with the processing interview, during the final interview the CI applicant should be afforded the opportunity to withdraw his packet from consideration to ensure the applicant is devoted to becoming a CI special agent.

A-12. **Processing CI applicant packet.** After the final interview is completed, the interviewing agent will prepare a statement of interview detailing the key points of the interview as well as his recommendation for approval or disapproval and the reasons why. A letter of transmittal will be prepared. The transmittal letter,

statement of interview, and all required documentation will be forwarded to the U.S. Army Human Resources Command (USAHRC). The interviewing agent will contact the applicant and the applicant's unit commander to inform them the packet has been forwarded to USAHRC. The interviewing agent should keep both the applicant and the commander informed as to the status of the process and when the final approval or disapproval is granted by HRC.

A-13. **On-the-job training (OJT).** Upon notification of acceptance into the 35L MOS, the CI applicant can request through his chain of command to attend OJT with the CI element that supported his CI applicant process. For OJT sessions lasting more than 6 months, attachment orders may be required. For OJT sessions shorter than six months, DD Form 1610 (Request and Authorization for TDY Travel of DOD Personnel) are not required but may be desired. The CI applicant can obtain an acceptance letter from the supporting CI office endorsing his request for OJT. During the OJT time, the CI applicant will remain assigned to his original unit; however, the CI element providing OJT will provide feedback and bullets for evaluations.

A-14. **Issuance of CI badge and credentials.** Newly certified CI special agents are NOT issued CI badge and credentials during or at the completion of the CI special agents course (CISAC). Their gaining unit will be responsible for submitting a request justifying the need for CI badge and credentials to the Army CI Badge and Credentials Program Office, INSCOM Training and Doctrine Support (ITRADS) Detachment, Fort Huachuca, AZ. ITRADS will adjudicate the request for issuance of the CI badge and credentials.

A-15. **Counterintelligence Probationary Program (CIPP).** All newly certified CI special agents are required to complete a one-year probationary period and be favorably recommended for retention in the Army CI Program by their unit commander. The CIPP period begins immediately upon reassignment to the first assignment in a CI position.

ARMY COUNTERINTELLIGENCE BADGE AND CREDENTIALS PROGRAM

A-16. The Army CI Badge and Credentials Program grants the bearer of the CI badge and credentials special recognition and bona fides during the conduct of official Army CI activities with other U.S. military and civilian governmental agencies. Because of the special access, official privileges and authority associated with possession of CI badge and credentials are considered sensitive items requiring the same strict issue, control, and accountability procedures afforded to weapons or cryptographic items.

A-17. The Army staff CI and HUMINT operations coordinator (G-2X) is the executive agent for the Army's CI Badge and Credentials Program. The Army G-2X is responsible for establishing policy governing the issuance, use, and accountability for CI badge and credentials. ITRADS, Fort Huachuca, AZ, is the program manager for the CI badge and credentials program.

A-18. Army CI badge and credentials are issued only to persons who—

- Have completed a CI qualification course approved by the DA G-2 for the issuance of CI badge and credentials.
- Have been awarded MOS 35L enlisted (formerly 97B), 351L warrant officers (formerly 351B), 35E officers and government civilians in occupation series 0132 (including Army civilians and members of the MI Civilian Excerpted Career Program [MICECP]).
- Are at least 21 years of age.
- Are assigned to a CI position requiring the use of CI badge and credentials to accomplish the unit's mission.

A-19. **Unit custodians.** All units who have assigned CI special agents are required to appoint both a primary and an alternate CI badge and credentials custodian. The CI badge and credentials custodian is responsible for—

- Implementing a suspense system for tracking and receipting for inbound CI badge and credentials materials, whether shipped or hand-carried to the unit.
- Receipting for CI badge and credentials materials, by badge and credentials control numbers, on the same day the CI badge and credentials materials arrive at the unit, whether shipped to the unit or hand-carried during reassignment.
- Coordinating hand-carry transfers, regardless of whether the agent wants to hand-carry, when the agent is being reassigned to a unit listed on the account custodian list.
- Inventorying all unit CI badge and credentials materials semiannually and when the unit's primary custodians change.
- Retaining all serviceable CI badge and credentials and representative credential cases for CI badge and credentials materials returned to ITRADS. Unserviceable cases should be cut in half and thrown away.

A-20. **Unit account holders.** Unit account holders are the commander or the C/J/G/S-2 of the unit. Unit account holders have the responsibility of—

- Ensuring that the unit has a primary and alternate CI badge and credentials custodian appointed on orders signed by the commander.
- Requesting the establishment of a CI badge and credentials account if there are CI special agents assigned to the unit or subordinate units for which the unit account holder is responsible.
- Coordinating with the CI badge and credentials program manager to revalidate CI badge and credentials accounts that have been suspended, de-activated, or otherwise in a dormant state.

COUNTERINTELLIGENCE BADGE AND CREDENTIALS INVENTORIES

A-21. Army CI badge and credentials consist of the following:

- **MI badge.** The MI badge has a control number stamped into the back; this is the number custodians report on receipts and inventories.
- **Intelligence credentials.** DA Form 3363 (US Army Intelligence Credential Special Agent), DA Form 3363A (US Army Intelligence Credential Representative), or DA Form 3363-1 (US Army Intelligence Credential Photograph /Signature). Each form has a 6-digit control number printed on the reverse side of the card; this is the number custodians will report on all receipts and inventories.

A-22. Custodians are required to conduct a 100 percent, hands-on, physical inspection and inventory of all CI badge and credentials materials issued to the unit's account. This is done semiannually and when the unit's primary custodian changes.

A-23. Semiannual inventories must be conducted every six months based upon the schedule produced by ITRADS and the results forwarded to ITRADS.

A-24. Change of custodian inventories require a joint inventory be conducted between the incoming and outgoing primary custodians. This joint inventory must be conducted and reconciled with ITRADS before the physical departure of the outgoing primary custodian, and must be signed by both the incoming and outgoing primary custodians.

A-25. Custodians may not conduct an inventory using on-hand receipts. When an individual issued CI badge and credentials materials is not present for an inventory (deployment, extended TDY, other), the custodian will contact that individual or another responsible person who can verify that the individual still has the items in his possession, and to confirm all appropriate control numbers to the custodian.

A-26. Inventories will be prepared in a roster (column) format, alphabetically, with separate columns for the agent's name, rank, badge number, and DA Forms 3363, 3363A, and 3363-1 numbers. If the unit is not responsible for representative credentials, then there will be no requirement for a DA Form 3363A column.

Note. Do not include social security numbers on inventories.

A-27. All inventories faxed to ITRADS must be signed by the custodian who conducted the inventory.

A-28. Because of the signature requirement for change of custodian inventories, they must be faxed to ITRADS. The signed inventory may be scanned and saved as a .pdf document (Adobe Acrobat readable).

A-29. When CI badge and credentials materials are transferred to another unit's account or returned to ITRADS, those items remain on the losing unit's inventory until the gaining unit's custodians or ITRADS receipts for the items.

A-30. The physical inspection of the CI badge and credentials materials is to ensure the badge is not worn, tarnished, or excessively bent. The credential forms will be inspected to ensure the lamination is not splitting or they are excessively scratched.

A-31. The unit's inventory will be compared against the Army's Central CI Badge and Credentials Repository database. Once the inventory is reconciled, ITRADS will send an email to the unit custodian confirming the reconciliation. The email will provide the month and year the unit's next semiannual inventory is due, and direct the custodian to print the inventory reconciliation email as the unit's official inventory reconciliation documentation. This email is required to be maintained on file by the unit until the next semiannual or change of custodian inventory is reconciled.

A-32. **Individual responsibilities.** Individuals issued CI badge and credentials are responsible for the safeguard, protection, accountability, and use of their CI badge and credentials. Although CI badge and credentials are issued from ITRADS to the individual's CI special agent based upon an operational requirement, unit SOPs may provide for more stringent controls, protection, and accountability of CI badge and credentials. CI badge and credentials are Army property. Personnel issued CI badge and credentials will—

- Use the CI badge and credentials in accordance with Army policy, doctrine, and unit SOPs to support their unit's mission.
- Protect and safeguard their CI badge and credentials to ensure accountability.
- Execute a statement acknowledging their responsibilities for the use and safeguarding of the CI badge and credentials when issued and reissued CI badge and credentials.
- Immediately report any misuse, loss, or theft of CI badge and credentials to the unit CI badge and credentials custodian.
- Coordinate with the unit CI badge and credentials custodian for the transport or transfer of CI badge and credentials upon notification of reassignment.
- Be knowledgeable of all policies and procedures for the use, protection, and accountability of CI badge and credentials.
- Surrender his CI badge and credentials to the unit CI badge and credentials custodian when going on leave, TDY, international travel, or any other absence that does not require the use of CI badge and credentials.

HAND-CARRYING COUNTERINTELLIGENCE BADGE AND CREDENTIALS

A-33. The following are custodian definitions:

- Losing unit custodians—custodians for the unit the agent is currently assigned to.
- Gaining unit custodians—custodians for the unit the agent is being reassigned to.

A-34. The Army may authorize agents to hand-carry, or physically take their CI badge and credentials during reassignments for the purpose of eliminating the agent's downtime at the gaining unit and to reduce postal expenses across the Army. Hand-carry transfers must be formally coordinated in accordance with the policies and procedures provided below. There are no "informally" coordinated hand-carry transfers.

- CI special agents will not permanent change of station (PCS) with CI badge and credentials without written authorization (email) from ITRADS.
- Hand-carry transfers must be coordinated if the agent is being reassigned to a unit that has an established CI badge and credentials account, and will be coordinated not earlier than 30 days out from the day the agent physically departs the unit. Hand-carry transfers will not be approved for agents who are being reassigned to a unit that does not appear on the account custodian list, which means the unit does not have a CI badge and credentials account.
- Agents do not have a choice whether they hand-carry their CI badge and credentials during reassignment. The hand-carry decision will be made during coordination between the custodians involved and ITRADS.

Note. If there are extenuating personal circumstances which may impact the agent's hand-carry, the unit custodian must bring it to the attention of ITRADS immediately. Depending on the situation, ITRADS may direct the losing unit to ship the agent's CI badge and credentials directly to the gaining unit's custodian.

- Hand-carry transfers will not be approved for agents who are attending a school, or who are going to be TDY en route.
- The gaining unit is not authorized to initiate the hand-carry email process; only the losing unit's custodians may initiate the hand-carry email coordination process.
- CI badge and credentials stay on the losing unit's inventory until the gaining unit's custodian sends a receipt to the losing unit's custodians and ITRADS. Therefore, if the losing unit sends an inventory to ITRADS before receiving a receipt from the gaining unit for the hand-carried CI badge and credentials, the hand-carried CI badge and credentials must still be included on the losing unit's inventory.
- Agents will not hand-carry CI badge and credentials without written (email) authorization from ITRADS.
- When agents are not authorized to hand-carry their CI badge and credentials, or when they are separated from Army service, the unit custodian is required to ship that agent's CI badge and credentials back to ITRADS as soon as the agent no longer needs his CI badge and credentials (for example, when the agent out-processes through the custodian).

TRANSFERRING COUNTERINTELLIGENCE BADGE AND CREDENTIALS

A-35. CI badge and credentials materials will be retrieved by the unit custodian and returned to ITRADS when the agent is being reassigned and not authorized to hand-carry. The custodian should retrieve these CI badge and credentials during the agent's out-processing and return them to ITRADS. Custodians will also expeditiously return CI badge and credentials for agents who have had their clearance formally suspended or revoked.

A-36. Custodians must include orders for all CI badge and credentials being returned to ITRADS. If CI badge and credentials materials are returned for reasons or situations for which orders are not generated, custodians will annotate on the return memorandum why the CI badge and credentials materials are being returned.

A-37. Custodians are ultimately responsible for ensuring that CI badge and credentials materials are shipped using one of the following postal services (Federal Express, registered, or Postal Express).

Note. This is Army policy. Custodians must ensure their unit mailrooms understand this requirement. Noncompliance with this requirement will be addressed to the unit's account holder for command involvement.

A-38. Custodians must include a receipt in all packages of CI badge and credentials shipped to ITRADS or another unit. The receipt will be an itemized list of all items within the package.

A-39. Upon receiving the CI badge and credentials materials, ITRADS will normally send the custodian an email receipt for the items. In the event ITRADS receives a large shipment of CI badge and credentials materials, the hardcopy receipt may be Faxed back to the unit custodian.

LOSS OF COUNTERINTELLIGENCE BADGE AND CREDENTIALS

WARNING

Loss of CI badge and credentials can be a basis for disciplinary action, removal of the CI MOS, or removal from CI duties.

A-40. In the event that CI badge and credentials are lost, the individual will immediately notify the account holder, the unit custodian, and their chain of command. A search will be immediately initiated in the area where the loss is suspected to have occurred.

A-41. If the CI badge and credentials are not recovered within 48 hours, the individual's commander will—

- Initiate an AR 15-6 investigation to ascertain the facts and circumstances surrounding the loss of the CI badge and credentials.
- Provide ITRADS with a memorandum formally reporting the loss of the CI badge and credentials.
- Notify local, state, and federal agencies in the area where the loss may have occurred and request assistance in recovering the CI badge and credentials.
- Upon completion of the AR 15-6 investigation, the account holder will provide ITRADS with a copy of the final report of investigation (ROI). The report will include—
  - The identity of the person who lost the CI badge and credentials.
  - All the facts and circumstances concerning the loss.
  - The investigating officer's determination as to whether the loss was the result of negligence.
  - Any administrative or judicial actions taken because of the loss.
  - A request for relief of accountability if the CI badge and credentials were not recovered.

MISUSE OF COUNTERINTELLIGENCE BADGE AND CREDENTIALS

A-42. Individuals are issued CI badge and credentials for the purpose of identifying themselves as CI special agents in an official capacity to other U.S. military and government agencies and HN agencies. CI badge and credentials are never to be used for personal gain or any other situation that is not directly associated with an official CI mission requirement. Misuse and/or abuse of CI badge and credentials can be the basis for disciplinary action, removal of the CI MOS, or removal from CI duties.

A-43. CI badge and credentials misuse and/or abuse include, but are not limited to—

- Use or display of CI badge and credentials for any purpose other than official business or an intelligence activity to support the unit's mission.
- Use or display of CI badge and credentials when another form of identification is appropriate for the situation (for example, to gain admittance to an installation when a military or civilian identification would be sufficient).
- Any falsification, forgery, reproduction, alteration, or tampering with CI badge and credentials, including copying the credential forms.
- Storing anything other than the badge and credential forms in the carrying case (for example, driver's license, business cards, currency).
- Transporting or removal of CI badge and credentials upon reassignment without prior coordination with the unit custodian and ITRADS.
- Any disregard for the policies and procedures specified in AR 381-20, this field manual, or the CI badge and credentials guide listed in this manual.

COUNTERINTELLIGENCE PROBATIONARY PROGRAM

A-44. The nature of CI requires that Army CI special agents must possess the highest levels of competence, maturity, and ethical and moral standards. The DOD Board of Investigations recognized this and mandated Army MI establish a formal, centrally supervised probationary program for Army CI special agents. Therefore, all newly trained CI special agent will participate in the CIPP for the first year in a CI assignment (enlisted, warrant officers, officers, and Army civilians, including members of the Army MICECP).

A-45. Following graduation from the CISAC, the CI special agent will be assigned to a CI position. The newly certified CI special agent will complete a one-year probationary period. During this time the CI special agent must demonstrate the technical competence and character traits to retain the 35L MOS. At the end of the probationary period, the first lieutenant colonel (O-5) in the chain of command will notify the USAHRC that the special agent has demonstrated the capability and competency to perform CI duties and has successfully completed the CIPP, or that the person has not demonstrated the abilities for continued service as a CI special agent and should not be retained in the MOS. At no time will the CIPP period exceed 18 months for Regular Army Soldiers and 24 months for Army National Guard (ARNG) Soldiers.

A-46. Supervisors of government civilian CI special agents will incorporate a condition of employment into the civilian job descriptions that requires satisfactory completion of the CIPP period within one year of assignment to a CI position. The CIPP for civilian CI special agents is separate from the one-year probation which is required of all newly hired Government civilian personnel.

A-47. The Government employment probation period is for the purpose of determining the person's suitability to work as a government civilian employee while the former is for the purpose of assessing the capability and competency of the civilian to perform CI duties. Failure of the latter will result in removal from government service. Failure of the former will allow the individual to apply for other government employment.

A-48. The CIPP applies to warrant officers/351L who were not issued CI badge and credentials during their previous enlisted or commissioned officer service.

A-49. The CIPP will assure the elimination, fairly and uniformly, of unsuitable personnel from the professional ranks of the Army CI. Commanders should not recommend acceptance of probationary CI special agents if they do not meet standards to perform as CI special agents.

A-50. ARNG organizations will require additional time for the CIPP period. The CIPP period will be a minimum of 18 months and must include 2 annual training periods. If individuals are activated for a CI special agent position, the CIPP period can be reduced to 12 months from their time of activation.

A-51. DCS G-2 is the Executive Agent for the CIPP and will assign an Army CIPP program manager (PM) for the implementation of the CIPP. The Army CIPP PM will—

- Publish guidance to commanders of CI special agents implementing the CIPP. Guidance will include the standards used to determine acceptance of individuals in the CIPP period.
- For each individual graduating from the CISAC course, will forward a memorandum to the first lieutenant colonel (O-5) in the individual's chain of command that outlines evaluation criteria, timeliness, and support available from the CIPP PM and USAIC&FH.
- Coordinate with the DCS G-2, USAHRC, and USAIC&FH to establish standards that guide commanders and unit CIPP managers in the evaluation of individuals in the CIPP.
- Be collocated with the Army CI badge and credentials PM, USAIC&FH.
- Coordinate with commanders' assigned Army CI special agents to ensure compliance with CIPP procedures and track professional and training development of individuals in the CIPP. As necessary, conduct inspections of commands assigned CI special agents to ensure compliance with procedures outlined in AR 381-20 and all applicable HRC regulatory requirements.

A-52. Commanders of CI special agents (first lieutenant colonel [O-5] in the chain of command) will—

- Comply with the guidance promulgated by AR 381-20, HRC guidance, and supplemental guidance established by the CIPP PM.
- Have at least 90 days to observe a CI special agent who is in the CIPP before evaluating and recommending retention or removal from the CI Program. If the certifying official does not meet this requirement, the CIPP period may be extended up to 15 months until the 90-day requirement is met.
- Ensure that all CI special agents in the CIPP are "partnered" with a senior CI special agent for professional development.
- Supervise the 12-month CIPP period, which requires enlisted, warrant officer, officer, and government civilians in the gaining unit to evaluate the potential of the CIPP individuals to perform the duties of a CI special agent. This evaluation includes periods of teaching, mentoring, and coaching by experienced CI personnel. The evaluation is divided into three areas: character, skills, and knowledge.

A-53. **Character.** Leaders will determine if the individual demonstrates responsibility, diligence, initiative, innovation, and self-reliance. Additionally, the CIPP individual's maturity, moral, and ethical attitudes should be factors for considerations.

A-54. **Skills.** The intent of the skills evaluation is to ensure an individual demonstrates those skills required to be a successful CI special agent. For individuals not assigned to units with an investigative mission, leaders will evaluate potential of the individual to be a professional CI special agent. In the latter situation, leaders and experienced CI personnel will evaluate the individual's ability to execute skills common to all the CI functions. These skills include—

- **Interpersonal skills**—the ability to relate to people and cause individuals to cooperate with the CI special agent.
- **Elicitation**—the ability to obtain information from people in a non-intrusive manner.
- **Questioning techniques**—the ability to directly obtain information from targeted individuals.
- **Writing**—the ability to accurately relate the information obtained.

A-55. Individuals that perform and satisfactorily demonstrate the above skills not only have the potential to be a technically competent CI special agent but a technically competent investigator. Performance evaluation and counseling every 90 days during the CIPP period is mandatory. The counseling should be

done by the senior CI special agent in the person's unit or higher headquarters who has direct access to observe and evaluate the person's training and performance. The performance evaluation and counseling will NOT be conducted by someone who is in the CIPP or has less than two years of experience (not including their CIPP participation) as a CI special agent. During any of the counseling sessions if the individual's performance is substandard, the details of the substandard performance must be given to the CIPP individuals in writing along with a performance improvement program of how to correct the deficiencies. It is incumbent upon the CI special agent's parent unit to provide mentorship, training, and materials to allow the person to successfully learn and demonstrate the ability to function as a CI special agent.

A-56. **Knowledge.** During the month preceding the final month of the CIPP period, CIPP special agents will be required to take a skills test to demonstrate their continued knowledge concerning specifics of the doctrinal execution of CI tasks including, but not limited to, CI-related regulations, intelligence law, and investigative procedures. The test will be administered by the installation education facility. The testing facility will forward the results of the test to the CIPP individual's chain of command and simultaneously to the CIPP PM. CIPP individuals who fail the test may be given a second opportunity within six months based upon a recommendation by the chain of command. The CIPP PM, with the USAIC&FH Training Development and Support Directorate, will establish the testing packet and make training aids available online.

A-57. Circumstances may arise that do not permit the CIPP period to be completed at the 12-month mark. Extensions may be granted beyond the original requirement based upon the submitting lieutenant colonel's (O-5's) time in position or due to deployment reasons. Request for extensions will be coordinated between the CIPP individual's parent unit and the CIPP PM on a case-by-case basis. At no time will the CIPP period exceed 18 months for Active Army Soldiers or 24 months for ARNG Soldiers.

A-58. The commander will—

- Appoint a unit CIPP PM in writing, in memorandum format, and forward a copy of the appointment orders to the CIPP PM, Fort Huachuca, AZ. The unit CIPP PM will be a senior warrant officer (351L) or senior NCO E-7 or above, (35L) who can track the arrival, departures of all CIPP individuals and coordinate with the unit plans and training element to ensure appropriate and effective training is considered, scheduled, and executed. A unit CIPP PM must have at least 2 years in the CI MOS (excluding his own CIPP period).
- Forward a signed memorandum to the CIPP PM, Fort Huachuca, AZ, and USAHRC concerning the results of the skills evaluation and a recommendation to retain or remove the CIPP individual from the CI MOS. If the CIPP individual is recommended for retention in the CI MOS, the 35L will be permanently awarded as the primary MOS. If removal from the CI MOS is recommended, the recommender may advise on an alternative MOS or Area of Concentration or duties in the recommendation packet. Failure to complete the CIPP period is not, by itself, considered to be an adverse personnel action.
- At the completion of the 12-month CIPP period, forward a recommendation packet to the CIPP PM, Fort Huachuca, AZ, and to USAHRC concerning the results of the skills evaluation and a recommendation to retain or remove government civilians in the CIPP from the CI MOS. Civilian supervisors will determine if the individual should be retained in government service.

A-59. DCS G-1 is responsible for—

- Establishing personnel management policy for CI special agents in the CIPP.
- Coordinating with the first O-5 in the CIPP individual's chain of command and Army CIPP PM that the CIPP individual has met the CIPP period, evaluation, and qualifications for permanent awarding of the CI MOS.

- Coordinating with the first O-5 in the CIPP individual's chain of command, the Army CIPP PM, and USAHRC for individuals not meeting the requirements and not being recommended for retention in the CI MOS.
- Coordinating with USHRC for re-classification procedures and orders to the appropriate training institution and follow-on assignment instructions.
- Establishing policies for appealing and adjudication for individuals who unsuccessfully complete the CIPP.

A-60. USAHRC is responsible for—

- Administering and supervising the personnel management aspects of the Army CI Program in accordance with DODR 5210.48 and 5240.5 and applicable Army regulations and personnel policy including the formal establishment of the Army CIPP for all newly trained CI special agents (enlisted, warrant officer, officer, and government civilians).
- In conjunction with USAIC&FH and the Army CIPP PM, tracking and evaluating CI candidates and assigned personnel whose applications or files indicate they may be unsuitable for the Army CI Program and accordingly approve or disapprove their assignment or continuation in the CI Program.
- Notifying DCS G-2 and Army CIPP PM of the award or removal of the CI MOS for all CI Program personnel and CIPP individuals.
- Furnishing copies of assignment orders or instructions for CI personnel to the Army CIPP PM.
- In conjunction with DCS G-1 developing policy concerning removal or retention of special bonuses or pay associated with unsuccessful completion of the CIPP and removal from the CI Program.

A-61. USAIC&FH is responsible for—

- Developing doctrinal literature and training materials for the Army CIPP including training support packages to enable commander's implementation of the CIPP.
- Developing online training materials to enable the unit CIPP PM to monitor CIPP individuals' aptitude and adjust unit training plans to effectively target areas that need more attention.
- Conducting formal CI training for enlisted, warrant officer, officer, and government service civilians accepted into the CI Program.
- Developing and updating the CI MOS evaluation test required in the month before the final month of the CIPP period.
- Creating an individual development plan for all new CI special agents.
- Developing a standard checklist for commanders, first-line supervisors and unit CIPP PMs concerning the expectations of a CI special agent during the CIPP.

Appendix B

Contractor Support to Counterintelligence Activities

Contractors are used increasingly to augment existing capabilities and bridge gaps in the deployed force structure. With the increased use of contractors comes the need to identify the doctrine and procedures affecting their employment. Leaders and those working with contractors must understand that contractors are civilians authorized to accompany the force in the field and should be provided with an identification (ID) card as proof of their authorization.

B-1. CI is considered inherently governmental work due to the constitutional issues associated with investigations, operations, and other activities of U.S. persons. The Army employs contractor personnel to execute specific, Government-controlled and supervised tasks, such as CI screening of potential linguists and staff work, but all operational actions are executed by Government personnel. Contractors cannot serve as credentialed CI special agents in the continental United States (CONUS) or outside the continental United States (OCONUS).

B-2. CI contractors may serve as screeners or debriefers, conducting personnel security investigations, functioning as intelligence or command staff members, and even working as analysts, but none are on Army CI "Investigative" status and will not be actively engaged in CI investigations or collection activities and operations.

TYPES OF CONTRACT SUPPORT

B-3. The various types of contract support are discussed below:

- **External support contractor.** Contract intelligence personnel fall into the category of external support contractor. They work under contracts awarded by contracting officers serving under the command and procurement authority of supporting headquarters outside the theater. Their support augments the commander's organic capability.
- **Contract CI staff member.** A contract CI staff member is a contractor who is specifically trained for, tasked with, and engages in normal staffing actions for Army commands, Army Service component commands (ASCCs), and Department of the Army (DA) G-2, such as coordinating regulations for publication and preparing memorandums for the commanding general to sign giving his major subordinate commanders guidance on certain issues. Other examples would include working staff officer positions in headquarter units at all levels or serving as reports officers to coordinate intelligence reports for publication to the intelligence community. Their operations must be conducted in accordance with all applicable U.S. law, treaties and conventions, and Army policies and regulations.
- **Contract CI analyst.** A contract CI analyst is a contractor who is specifically trained for, tasked with, and engages in analytic efforts to support intelligence requirements and analysis. They may also be tasked to search the Internet, Secure Internet Protocol Network (SIPRNET), and Joint Worldwide Intelligence Communications System (JWICS) to support CI investigations and collection and organize large amounts of data to help the investigator make sense of that information. Their operations must be conducted in accordance with all applicable U.S. law, treaties and conventions, and Army policies and regulations.
- **Contract security investigator.** A contract security investigator is a contractor who is specifically trained for, tasked with, and engages solely in the conduct of personnel security investigations. Their credentials are issued from the Office of Personnel Management (OPM)

or the Defense Security Service (DSS) and do not grant them authority to conduct any type of CI investigative actions.

- **CI contract screener or debriefer.** A contract screener or debriefer is a contractor who is specifically trained for, tasked with, and engages in the screening or debriefing of locally employed personnel (LEP). There have been cases where contractors have been used in CI screening roles for LEP, but this is more of a debriefing role than a CI-specific mission or role. Their operations must be conducted in accordance with all applicable U.S. law, treaties and conventions, and Army policies and regulations.
- **Contract linguist.** A contract linguist is a contractor who is specifically trained for, tasked with, and engages in interpreter or translation activities. Linguists or translators may be employed, once properly hired and vetted by appropriate personnel for CI and criminal issues at a minimum, under the direct supervision of an active duty or government person in accordance with the terms and conditions of their contract. Their operations must be conducted in accordance with all applicable U.S. law, treaties and conventions, and Army policies and regulations.

CIVILIAN STATUS

B-4. Contract employees cannot be made to engage in any activity inconsistent with his civilian status, such as serving as a crew member on a weapon system. Analysis and staff position responsibilities and functions are presumptively consistent with civilian contractor status, but other tasks should be vetted with the command's legal advisor to ensure they are legally permissible. For further information, see FM 3-100.21.

Appendix C

Interpreter Support to Counterintelligence Activities

The use of interpreters is a significant part of the counterintelligence (CI) investigative, operational, and collection efforts. Therefore, it is vital that the CI special agent be provided access to a qualified pool of interpreters. These can be Army linguists, contract linguists, or properly screened and vetted local national employees. Use of an interpreter is time consuming and potentially confusing; therefore it is vital that sufficient time is allowed for familiarization and mission briefs between the agent and the supporting interpreter.

C-1. Proper use and control of an interpreter is a skill that must be learned and practiced to maximize the potential of CI collection. It is also vital for the CI special agent to confirm that the interpreter he intends to use actually holds the required clearance for the level of information that will be discussed or potentially collected, and is authorized access to either the facility, compound, subject or suspect, or source.

C-2. This chapter deals strictly with the use of interpreters to support CI investigations, operations, and collections and is not intended to be applied to more routine uses of interpreters to support administrative, logistic, or other operational requirements.

ADVANTAGES

C-3. Interpreters are often a necessary aid to successful CI investigations, operations, or collection activities conducted outside the continental United States (OCONUS). There are certain advantages to using an interpreter; the most obvious is that without an interpreter, a CI special agent without the proper language or necessary proficiency in the target language is severely limited. Furthermore, if properly trained, briefed, and prepared, the interpreter can provide invaluable assistance to the CI special agent during the conduct of his mission. This is frequently the case because the interpreter—

- Likely has a greater knowledge of the local culture and language usage than could be developed by the CI special agent.
- Can identify language and culturally based clues that will help the CI special agent confirm or refute the veracity of the source's statements.
- Can interpret not only the literal meaning of a statement but also the intent and emotion of a sentence as well as periods of silence and other nonverbal clues.

DISADVANTAGES

C-4. There are several significant disadvantages to using interpreters; for example:

- There is a significant increase in time to conduct the activity. Since the interpreter must repeat each phrase, the time for an interview session, liaison, or meeting can be easily doubled.
- The potential for confusion or misunderstanding increases significantly when there is a third person in the communications loop. This is especially true when the interpreter is deficient in his command of either the target language (based on dialect or education level) or English.
- The establishment of rapport and the use of effective elicitation or questioning techniques are made difficult or even impossible when working through an interpreter based on unwillingness to use them or a lack of familiarity and appreciation of the subtleties and nuances required to employ them effectively.

- The ability of the CI special agent to interpret the source's veracity through the analysis of word usage, nuances of speech, and body language is curtailed.
- Interpreters will have their own set of biases that could influence the manner in which the dialogue is interpreted and reported back to the CI special agent.
- The source may be culturally biased against the interpreter. This is especially possible if the interpreter was locally hired and is of a different ethnic, social, or religious group than the source.
- There may be mission or subject matter problems involved as the interpreter may not be familiar or conversant in some of the more technical aspect of the subject area.

PRECAUTIONS

C-5. CI special agents should be cautious of making seemingly innocuous comments in the presence of interpreters and always remember that the interpreter is not a friend or even an ally. Interpreters are being paid to perform a service and although they have been vetted, agents can never completely trust the interpreter. CI special agents must create a thorough interview plan with the help of the interpreter, but agents must still only share needed information so the interpreter functions effectively. Need-to-know concerns apply everywhere to everyone but especially to the interpreter.

C-6. The exchange of information regarding the basic interrogatives (*who*, *what*, *where*, *when*, and *why*) of each meeting must be discussed with the interpreter only to the point of understanding the mission. The real "why" is likely none of the interpreter's business. CI special agents may be meeting with a source or contact because the commander believes this individual has lied. The real purpose (the *why*) of the meeting is to pose control questions and to determine whether the source or contact lied in the past or whether there was simply a miscommunication. Special agents may have suspicions regarding the very interpreter they are working with, and this is an attempt to ascertain the interpreter's veracity. As with all CI activities, a healthy dose of skepticism is required to maintain an advantage against the adversary.

C-7. Be careful of sensitive or personal conversations when the interpreter is in the area. This applies to conversations en route to or from meetings, conversations over lunch or dinner in the operational area, and conversations in the team area. It is easy to become accustomed to the presence and usefulness of an interpreter and to overlook the interpreter's presence. Interpreters are often a necessary tool but they are only lightly screened for the sensitive access they have. If the interpreter turned out to be working for the other side, what information beyond "the necessary" could the interpreter provide?

METHODS OF INTERACTION

C-8. There are two methods of interaction between the CI special agent and the interpreter: basic and advanced. As the CI special agent and the interpreter become experienced at working together and gain confidence in each other's abilities, they may use more advanced interactive techniques. It is the CI special agent's decision whether or not to use more advanced techniques.

BASIC INTERACTION METHOD

C-9. The basic method of interaction is used when—

- The interpreter and CI special agents have not worked together extensively.
- The interpreter has language skills but no interpreter training or experience.
- The interpreter's skill in English or the target language is suspect.
- The CI special agent has limited experience using an interpreter.
- The interpreter's capabilities, loyalty, or cultural knowledge are not known or suspect.

C-10. Using the basic method, the interpreter is used solely as an interpretation device. When initial contact is made, the interpreter instructs the source to maintain eye contact with the CI special agent. The interpreter is briefed on the general course of the interview or collection activity but is usually not informed of the specific purpose or collection goals. While the interpreter will be instructed to reflect the attitude, behavior, and tone of voice of both the CI special agent and the source, the interpreter is told not to interpose comments or personal opinions in the conversation at any time during the operation. Likewise, the interpreter should have been informed not to stray from the topic, to ask the questions exactly as asked, and to report exactly as the source reports.

C-11. The questioning phase is conducted in the same manner as if no interpreter were used, with the obvious increase in time due to the interpretation. The interpreter uses the same person and tense as the CI special agent or source and does not add or subtract anything from the dialogue. The interpreter tries to fade into the background. The CI special agent should ensure that questions are focused on the source not to the interpreter. The source should likewise answer to the CI special agent, not to the interpreter. When reports are written, the interpreter will only be asked questions based on the actual translation of the dialogue.

ADVANCED INTERACTION METHOD

C-12. The advanced method of interaction requires additional training on the part of the CI special agent and the interpreter, extensive experience working together, and a rapport between the CI special agent and the interpreter. The CI special agent must trust both the capabilities and the judgment of the interpreter. At this level of interaction, the interpreter becomes a more active participant in the interview. The CI special agent remains in charge and it is made it clear to the interpreter that the CI special agent is responsible for the substance and direction of the questioning. The interpreter may be briefed as to the specific goals of the collection as this will aid greatly in the thoroughness of the questioning and the interpreters ability to ferret out and exploit the seemingly innocuous details and nuances that may have been otherwise overlooked.

C-13. The interpreter becomes a more active participant in the approach and termination phases to the point of even making planned comments to the source supportive of the CI special agent's approach. For example, if the CI special agent is using an incentive approach, the interpreter in an aside to the source can tell him that the CI special agent always keeps promises. This type of technique should only be used if both planned and rehearsed.

C-14. During the questioning phase, the interpreter supports the special agent by not only translating the word of the source but also cueing the CI special agent when there are language or culturally based nuances to what the source is saying that might add credence or doubt as to the veracity of the statements. For example:

- The interpreter could point out that although the source claims to be a factory worker, but the language the source uses indicates that the source has a university education.
- The interpreter could indicate that the dialect or pronunciation that the source is using does not match the area that the source claims to be from. During report writing, the interpreter supports the CI special agent by not only answering questions on the literal interpretation but also by adding, when appropriate, comments on the significance of both what was said and how it was said.

C-15. There are almost never sufficient interpreters to meet all mission requirements, considering interpreters used to support CI investigations, operations, or collection activities will require additional screening, a security clearance, and functional knowledge of the operational situation before employment. While a qualified interpreter can be used to support CI missions, the CI special agent can maximize the potential return on any mission if the interpreter has received specific training, is afforded the opportunity to work with the same CI special agent or team on a regular basis, and is treated with proper respect and courtesy.

C-16. The number of interpreters needed to support a CI collection mission is driven by the mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC) factors based primarily on the number of CI special agents, the dispersion of the CI special

agents or CI teams in the area of intelligence responsibility, and the number of interview, investigations, and missions to be accomplished. Normally one interpreter for every two nonlanguage qualified CI special agents is sufficient; however, in situations where a large number of high-value sources must be questioned in a limited time, a ratio of one-to-one may be required.

MILITARY INTERPRETERS

C-17. There are many Soldiers who have native language capabilities due to their heritage, culture, background, or upbringing. Ideally, their parent unit will have identified this special ability and sought to maximize their Soldier's potential by referring them for language testing, advanced training, or reclassification into a language-dependent or supporting MOS. Or these Soldiers will have volunteered their abilities when a contingency arises. The Army National Guard (ARNG) and U.S. Army Reserve (USAR) also have trained translators and interpreters, who may be deployed to serve as interpreters for the CI collection effort.

CIVILIAN INTERPRETERS

C-18. Civilian corporations may be contracted by the military to provide interpreters for an operation. These interpreters are divided into three categories:

- **CAT I linguists.** CAT 1 linguists are locally hired personnel with an understanding of the English language. They undergo a limited screening, are hired in-theater, do not possess a security clearance, and are used for unclassified work. During most operations, CAT I linguists are required to be re-screened on a scheduled basis. CAT I linguists should not be used for CI collection operations.
- **CAT II linguists.** CAT II linguists are U.S. citizens who have native command of the target language and near-native command of the English language. They undergo a screening process, which includes a national agency check (NAC). Upon favorable findings, these personnel are granted a secret collateral clearance. CAT II linguists are the most used by CI special agents.
- **CAT III linguists.** CAT III linguists are U.S. citizens who have native command of the target language and native command of the English language. They undergo a screening process that includes a special background investigation (SBI) and a polygraph. Upon favorable findings, CAT III linguists are granted a top secret (TS) clearance and an equivalent of a TS clearance. CAT III linguists are used mostly for high-ranking official meetings and by strategic CI special agents.

INTERPRETATION TECHNIQUES

C-19. During the planning and preparation phase of the CI collection, the CI special agent, in collaboration with the interpreter, selects a method of interpretation. There are two primary methods:

- **Alternate interpretation.** The interpreter listens to the entire phrase, sentence, or paragraph. The interpreter then translates it during natural pauses in speech.
- **Simultaneous interpretation.** The interpreter listens to the source and translates what he says, just a phrase or a few words behind. The CI special agent should select the simultaneous method only if all the following criteria are met:
  - The sentence structure of the target language is parallel to English.
  - The interpreter can understand and speak English as well as the target language with ease.
  - The interpreter has special vocabulary skills for the topics to be covered.

- The interpreter can easily imitate the CI special agent's tone of voice and attitude for the approaches and questioning technique selected.
- Neither the special agent nor the interpreter tends to get confused when using the simultaneous method of interpretation.

C-20. If any of the above-mentioned criteria in the simultaneous method cannot be met, the CI special agent should use the alternate method. The alternate method should also be used when a high degree of precision is required.

TRAINING AND BRIEFING THE INTERPRETER

C-21. The CI special agent will need to train an individual who has no interpreter experience as well as remind a trained interpreter of the basic interpreter requirements:

- Statements made by the interpreter and the source should be interpreted in the first person, using the same content, tone of voice, inflection, and intent. The interpreter must not interject his own personality, ideas, or questions into the interview.
- The interpreter should inform the CI special agent if there are any inconsistencies in the language used by the source. The CI special agent will use this information in the assessment of the source.
- The interpreter needs to assist with the preparation of reports and administrative documents relevant to the source and meeting.

C-22. Once the CI special agent has chosen a method of interpretation, the agent must brief the interpreter. This briefing must cover:

- The current situation.
- Background information on the source as available.
- The administrative particulars of the meeting such as where it will be held, the room set up, how long it will last.
- The specific positioning of the interpreter, the special agent, and the source being interviewed.
- The general or—if advanced method of interaction is being used—the specific collection objectives.
- Any special topic or technical language that is anticipated. If time allows, the interpreter should research any anticipated technical vocabulary with which he is unfamiliar.

C-23. Throughout the briefing, the CI special agent should fully and clearly answer any pertinent questions that the interpreter may have. Again, this is done with the operations security (OPSEC) and the principles of security and need to know firmly in hand. This helps ensure the interpreter completely understands his role in the CI collection process. With a more advanced interaction plan, the CI special agent and the interpreter should war-game their plan, consider alternatives routes to the same answer, and consider any likely contingency situations that may arise. Rehearse as time and circumstances allows.

PLACEMENT OF THE INTERPRETER

C-24. The interpreter should be placed in a position that enhances the mood or general impression that the CI special agent wants to establish. When dealing with persons of CI interest, sources, or subjects of investigations, the CI special agent should establish a dominant position, maintain a direct relationship with the source, and increase or at least maintain the current anxiety level of the source. For example:

- Having the CI special agent and the source facing each other with the interpreter located behind the source normally facilitates this. It also allows the CI special agent to maximize control of both the source and interpreter.
- If desired, having the interpreter enter the room after the source, so the source never sees the interpreter, can further heighten the anxiety of the source.
- Having the interpreters sit to the side of the CI special agent creates a more relaxed atmosphere and is the preferred position when conducting debriefings and official meetings.
- Having the interpreter at his side also facilities "off line" exchanges between the CI special agent and the interpreter.
- The special agent should avoid having the interpreter sit beside the source since this has a tendency of establishing a stronger bond between the source and the interpreter and makes "off line" comments between the special agent and the interpreter more difficult to execute.

C-25. When conducting source meetings in a public setting, a more natural appearance is desirable. The seating needs to conform to the norm at the location where the meeting is taking place. For example, if meeting at a restaurant, the CI special agent, interpreter, and source will sit naturally around the table.

INTERACTIONS WITH AND CORRECTION OF THE INTERPRETER

C-26. The CI special agent must control the interpreter at all times. The agent must be professional but firm and establish who is in charge. This is best accomplished before the conduct of the actual mission. During a questioning session, the CI special agent corrects the interpreter if violations of any standards, covered in the premission briefing, occur. For example, if the interpreter interjects ideas into the meeting, the interpreter must be corrected. Corrections should be made in a low-key manner as to not alienate the interpreter, interrupt the flow of the questioning, or give the source the impression that there is an exploitable difference of opinion between the CI special agent and the interpreter. At no time should the CI special agent rebuke the interpreter sternly or loudly while they are with the source.

C-27. The special agent should never argue with the interpreter in the presence of the source. If a major correction must be made, the CI special agent should temporarily terminate the meeting and leave the site temporarily to make the correction. The CI special agent needs to document any difficulties as part of his interpreter evaluation. The CI special agent must always ensure that the conduct and actions of the interpreter are within the bounds of all other governing agreements, regulations, laws, and guidelines.

C-28. The CI special agent must be alert for any signs that the interpreter is not performing as required. The following are some indicators of possible problems:

- **Long-to-short.** If the CI special agent takes 20 seconds to express a statement or question, and the interpreter reduces it to a 3-second translation, it may indicate that something has been omitted. The agent should not proceed until the issue has been resolved There is nothing wrong with stating that the interpreter is to translate everything that was just expressed. If the interpreter is properly trained, this should not be an issue. If this issue arises, despite the interpreter's training, then it has significance and must not be ignored.
- **Short-to-long.** If the CI special agent takes five seconds to express a statement or question, and the interpreter expands it to a 30-second translation, it may indicate that something has been added. The agent should not proceed until the issue has been resolved.
- **Body-language shift.** If the interpreter's body language suddenly and significantly shifts from normal behavior, the CI special agent should determine the reason. It is advisable for the agent to determine a baseline of behavior for the interpreter to facilitate recognition of changes. Perhaps the interpreter is reluctant to translate what the agent said. Be aware that the body shift indicates something is happening—find out what it means.

- **Unusual pauses.** Look for a longer delay than usual before the translation begins. Unless it is a vocabulary or concept issue, the long delay means that the interpreter is "thinking" before translating. Any thinking beyond what is needed to translate, as closely as possible, what was just said represents a potential problem. Again, the CI special agent should establish a baseline of behavior for the interpreter in order to recognize these unusual pauses.
- **Inappropriate reactions.** If the CI special agent says something humorous that should provoke a positive response from the source, and after the translation, the agent does not get that response, then the agent should wonder if the message got through. If the source becomes upset in response to something said positively, then the agent should begin to wonder what message was passed by the interpreter—did the agent fail to communicate clearly, or was it an accidental or deliberate mistranslation?

INTERPRETER SUPPORT IN REPORT WRITING

C-29. The interpreter assists the CI special agent in preparing all required reports. The interpreter may be able to fill gaps and clarify unclear details in the CI special agent's case notes. The interpreter may also assist in transliterating, translating, and explaining foreign terms.

EVALUATING THE INTERPRETER

C-30. After submitting all reports, the CI special agent evaluates the performance of the interpreter. This should be done in writing, and copies should be given to the interpreter and placed on file with the individual managing the CI collection portion of the interpreter program. The interpreter program manager needs to develop a standard evaluation format for inclusion in the unit standing operating procedure (SOP). The evaluation should note, at a minimum, the following points:

- Administrative data (date, time, interpreter's name).
- Language proficiency.
- Strengths and weaknesses of the interpreter with any problems and corrective actions taken.
- Type of interpretation used (simultaneous or alternate).
- Type of CI activity the interpretation was supporting (that is, an investigation, interview, debriefing, liaison meeting).
- Ability or lack of ability of the interpreter to use specific technical language that may have been required.
- Name of the CI special agent conducting both the interview and the evaluation.

C-31. The interpreter program manager uses the above formats to decide on future use of the interpreters, to develop training programs for the interpreters, and to assign interpreters to make maximum use of their specific capabilities. The CI special agent should also review interpreter personnel files before using an unfamiliar interpreter.

INTERPRETER SECURITY ASSESSMENT

C-32. Interpreter support is crucial to successfully executing CI operations in many foreign and contingency operations locations. CI operations require that all supporting interpreters be assessed to ensure they are reliable and can be trusted with classified and sensitive information concerning intelligence information and CI methods of operations. Most CI operations will employ CAT II linguists who are U.S. citizens and have a secret clearance. However, the interpreter may volunteer or be forced to cooperate with hostile or adversarial elements which may compromise CI operations and endanger the physical safety of the CI special agent.

C-33. In some instances interpreters may have cultural, ideological, political, or religious beliefs which they sympathize and identify with. This may motivate the interpreter to voluntarily cooperate with

segments of the host-nation (HN) government, populace, or elements hostile to the presence of U.S. forces. In other cases the interpreter may still have family, friend, and business associations in the area of operations (AO). In this case, the interpreters may be coerced or forced to cooperate with these groups or people due to threats against their family. Regardless of the motivating factors, all interpreters supporting CI operations should be thoroughly and continuously assessed to ensure they are not compromising CI operations purposefully or through negligent actions.

C-34. Security assessments of interpreters should be planned and compartmented to avoid alerting the interpreter or other interpreters. Security assessments should be conducted to ensure the interpreter is accurate, non-biased, not falsifying information obtained from a source and not relating untruthful statements from the CI special agent to the source during CI operations.

C-35. Assessments should be conducted to identify any CI flags or indicators that the interpreter is not credible, loyal, or may be working at the behest of another organization. If the assessment indicates any negative character or reliability issues, the CI element should take steps to unobtrusively restrict access while assessing whether the interpreter could be used in a CI operation to exploit the situation or whether to neutralize the threat through employment termination or prosecution. There are numerous ways interpreters can be assessed. Regardless of what type of assessment is used, the CI element should consult their staff judge advocate (SJA) for legal and contractual considerations that may affect or prohibit this type of assessment. The following examples of interpreter assessments are not all inclusive:

- **Monitoring.** The actions and conversations of an interpreter may be video or tape recorded during CI operational activity (interviews, debriefings, screenings, and elicitation) and later reviewed by a credible interpreter, ideally a CI special agent who is thoroughly proficient in the target language. This allows for a very discreet assessment and may also allow the CI element to have multiple assessments by different linguists to refute, mitigate, or corroborate the findings.
- **Polygraph.** CI elements can request polygraph support through their CI coordinating activity (CICA) to conduct counterintelligence scope polygraph examinations (CSPEs) to assess the credibility of an interpreter. CSPEs need to be compartmented until the time of the examination to ensure the interpreters do not attempt to avoid or make excuses for taking the examination or cause any hostility among other interpreters that may impact the assessment process.
- **Concealed evaluation.** Concealed evaluation is using another CI special agent who is thoroughly proficient in the target language to pose as a non-linguist to evaluate the interpreter during CI operations. The CI element should use a CI special agent from another unit who is unknown to the interpreter and who does not know the interpreter. This affords the CI element to portray the CI special agent as a newly arrived Soldier; it also allows the CI special agent to evaluate interpreters without any bias while at the same time not alerting the interpreters that they are being evaluated.

MANAGING AN INTERPRETER PROGRAM

C-36. Units requiring interpretation support need to identify an individual or individuals to manage the interpreter program. In most units, this will be someone in the G-2/S-2 section. The functions of the interpreter program manager (PM) include but are not limited to—

- Consolidating and prioritizing interpreter requirements.
- Coordinating with the G-1/S-1 to identify personnel in the unit with language skills who can be used as interpreters.
- Coordinating with the G-1/S-1 and G-5 to obtain qualified interpreters.
- Coordinating with G-2/S-2 for clearances, screening, and vetting of interpreters and potential interpreters.

- Coordinating with the G-3/S-3 to establish training for both the interpreters and those that will be using interpreters.
- Coordinating with the G-3/S-3 for language testing of the interpreters in both English and the target language as required.
- Coordinating with the G-1/S-1 and G-4/S-4 to ensure that all administrative and logistical requirements for the interpreters are met.
- Establishing and maintaining the administrative, operational, and evaluation files on the interpreters.
- Assigning or recommending the assignment of interpreters to operational missions based on their specific capabilities.

This page intentionally left blank.

Appendix D

FBI Delimitations Agreement

This appendix provides the content of the agreement governing the conduct of the Department of Defense (DOD) counterintelligence (CI) activities with the Federal Bureau of Investigation (FBI).

(U) SECTION 1.

(U) PURPOSE:

(U) The purpose of this memorandum is to establish jurisdictional boundaries and operational procedures to govern the conduct of counterintelligence (CI) activities by the military CI services of the Department of Defense (DOD) with the Federal Bureau of Investigation (FBI). It implements Executive Order (EO) 12036 § 1-1104, requiring procedures to govern the coordination of military CI activities within the United States; and supersedes the Delimitations Agreement of 1949, as amended.

(U) SECTION 2.

(U) DEFENSE COMPONTENTS AUTHORIZED TO CONDUCT CI ACTIVITES:

(U) Within the DOD, each of the military departments is authorized by EO 12036 to conduct CI activities within the United States in coordination with the FBI and abroad in coordination with the Central Intelligence Agency (CIA). Within the military departments, the Army Intelligence and Security Command (INSCOM), the Naval Investigative Service, and the Air Force Office of Special Investigations (AFOSI) are authorized by departmental regulation to conduct such activities. The term “military counterintelligence service” or “military CI service,” as used herein, refers to these components.

(U) SECTION 3.

(U) FEDERAL BUREAU OF INVESTIGATION COORDINATION WITH THE DEPARTMENT OF DEFENSE:

A. (U) Policy matters affecting DOD CI components will be coordinated with the Office of the Under Secretary of Defense for Policy.

B. (U) When a CI activity of the FBI involves DOD military or civilian personnel of the DOD, the FBI shall coordinate with the DOD (EO 12036 § 1-1104) for DOD personnel involvement. For other civilian personnel of the DOD, coordination shall be effected with the Office of the Under Secretary of Defense for Policy.

C. (U) It is contemplated those representatives of the field elements of the FBI and military CI services will maintain close personal liaison and will meet frequently and routinely for the purpose of ensuring close cooperation in carrying out their CI activities.

Figure D-1. FBI delimitations agreement contents

(U) SECTION 4.

(U) DEFINITIONS:

A. (U) The term “coordination” means the process of eliciting objections and comments prior to undertaking a proposed action. As used here, the term implies that no such action will be taken so long as the party with whom the action in question is raised continues to have objections that cannot be resolved.

B. (U) The term “counterintelligence” is included in the term “counterintelligence,” as defined in EO 12036 § 4-202, and refers to the systematic collection of information regarding a person or group which is, or may be, engaged in espionage or other clandestine intelligence activity, sabotage, international terrorist activities, or assassinations, conducted for, or on behalf of, foreign powers, organizations, or persons.

C. (U) The term “counterintelligence operations” is included in the term “counterintelligence,” as defined in EO 12036 § 4-202, and refers to actions taken against hostile intelligence services to counterespionage and other clandestine intelligence activities damaging to the national security.

D. (U) The term “DOD civilian personnel” includes all U.S. citizen officers and employees of the DOD not on active military duty and all foreign nationals employed by the DOD.

E. (U) The term “security service” refers to that entity or component of a foreign government charged with responsibility for counterespionage or internal security functions of such government.

F. (U) The term “United States” includes the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and all territories, possessions, or protectorates under U.S. sovereignty or control; but does not include occupied territory governed under the President’s authority as Commander in Chief.

(U) SECTION 5.

(U) POLICY:

A. (U) The responsibilities of each military CI service and the FBI for the conduct of CI investigations and operations shall be governed by relevant statutes, EO 12036, and this agreement.

B. (U) Each military department is responsible for protecting its personnel and installations for physical threats and for ensuring that its programs and activities which involve the national security are not compromised to hostile intelligence agencies.

C. (U) Within the United States, the FBI conducts CI and coordinates the CI activities of other agencies.

D. (U) Under combat conditions or other circumstances wherein a military commander is assigned responsibility by the President for U.S. Government operations in a particular geographic area, he shall have the authority to coordinate all CI activities within such area, notwithstanding the provisions of this memorandum, subject to such direction as he may receive from the Secretary of Defense.

E. (U) The military CI Services and the FBI are mutually responsible to ensure that there is a continuing and complete exchange of all CI information and operations data relevant to the particular concerns of each operating agency.

Figure D-1. FBI delimitations agreement contents (continued)

F. (U) Policy issues arising in the course of CI activities which cannot be resolved at the FBI, military CI service local or headquarters level shall be jointly referred to the Attorney General and the Secretary of Defense for resolution, or referred to the Special Coordination Committee (Counterintelligence) of the National Security Council in accordance with Special Coordination Committee guidelines.

(U) SECTION 6.

(U) DELINEATION OF RESPONSIBILITY FOR COUNTERINTELLIGENCE INVESTIGATIONS:

(U) Responsibility for CI investigations shall be appointed between the FBI and the military CI services of the DOD as follows:

A. (U) All investigations of violations of the Atomic Energy Act of 1946, which might constitute a CI investigation as defined herein, shall be the responsibility of the FBI regardless of the status or location of the subjects of such investigations.

B. (U) Except as provided by paragraph C(2) below, all CI investigations of foreign nationals undertaken within the United States shall be the responsibility of the FBI.

C. (U) CI investigations within the United States shall be conducted in accordance with the following jurisdictional guidelines:

1. (U) Except as provided herein, investigations of all civilians, including DOD civilian personnel, shall be the responsibility of the FBI.

2. (U) Investigations of U.S. military personnel on active duty shall be the responsibility of the CI service of the appropriate military department.

3. (U) Investigations of retired military personnel, active and inactive reservists, and National Guard members shall be the responsibility of the FBI; provided, however, that investigations of actions which took place while the subject of the investigation was, or is, on active military duty shall be conducted by the CI service of the appropriate military department.

4. (U) Investigations of private contractors of the DOD, and their employees, shall be the responsibility of the FBI. Provided, however, that nothing contained in this paragraph shall prevent the military CI services of the DOD, in a manner consistent with applicable Law and Executive Branch policy, from undertaking:

(a) (U) In those cases where the FBI chooses to waive investigative jurisdiction, investigative actions which are necessary to establish or refute the factual basis required or an authorized administrative action, to protect the security of its personnel, information, activities, and installations; or

(b) (U) To provide assistance to the FBI to support any CI investigation for which the FBI is herein assigned responsibility.

D. (U) CI investigations outside the United States shall be conducted in accordance with the following guidelines:

1. (U) Investigations of military personnel on active duty shall be the responsibility of the military counterintelligence services of the Department of Defense.

Figure D-1. FBI delimitations agreement contents (continued)

2. (U) Investigations of current civilian employees, their dependents, and the civilian dependents of active duty military personnel shall be the responsibility of the military CI services, unless such responsibility is otherwise assigned pursuant to agreement with the host government, U.S. law, or executive directive.

3. (U) Investigations of retired military personnel, active and inactive reservists, National Guard members, private contractors and their employees, and other U.S. persons, who permanently reside in such locations shall be undertaken in consultation with the FBI, CIA, and host government as appropriate.

4. (U) Provided, however, that nothing contained in this paragraph shall prevent the military CI services of the DOD, in a manner consistent with applicable law and executive branch policy from undertaking:

(a) (U) Investigative actions which are necessary to establish or refute the factual basis required for an authorized administrative action, to protect the security of its personnel, information, activities, and installations.

(b) (U) To provide assistance to the FBI or security service of a host government to support CI investigations outside the United States for which DOD is not herein assigned investigative responsibility.

(U) SECTION 7.

(U) COORDINATION OF COUNTERINTELLIGENCE OPERATIONS:

(U) (The procedures governing the coordination of CI operations within the United States by the military CI service with the FBI are contained in the classified annex to the memorandum.)

A. (U) The policy and procedures set forth herein shall be implemented in the regulations of the affected agencies.

B. (U) The provisions of this memorandum, and the classified annex made a part hereof, shall be effective immediately upon execution by the Attorney General and Secretary of Defense.

(original signed)	(ORIGINAL SIGNED)
Attorney General of the United States	Secretary of Defense
Date: 4/5/79	Date: 9 February 1979

Figure D-1. FBI delimitations agreement contents (continued)

Appendix E

Counterintelligence Investigative Report Writing Guide

E-1. Appendix E provides guidance on CI investigative report writing principles. The following are documents commonly used in CI investigative report writing:

- Table E-1. Personal data.
- Table E-2. Military ranks and civilian titles.
- Table E-3. Physical description.
- Figure E-1. CI incident report.
- Figure E-2. Investigative memorandum for record (IMFR)—interview.
- Figure E-3. Investigative memorandum for record—personnel files checks.
- Figure E-4. Investigative memorandum for record—records checks.
- Figure E-5. Investigative memorandum for record—intelligence files checks.
- Figure E-6. Investigative memorandum for record—law enforcement records checks.
- Figure E-7. Transmittal letter for report of investigation (ROI).
- Figure E-8. Report of investigation.
- Figure E-9. Summary of information (SOI).
- Figure E-10. Privacy Act of 1974 Advisement Statement.
- Figure E-11. Perjury warning.
- Figure E-12. Secrecy affirmation statement.

FORMAT RULES

E-2. **Font/Pitch.** Type all reports in Arial font, font size 12. CI special agents must write all investigative reports in a narrative format using third person, simple past tense, and active voice (Jones secured the document in the security container.). The only exceptions to this are the mandatory sentences adopted for use Army-wide in CI investigative reports, when quoting the source, indicating a state of mind or condition, or when describing attachments.

E-3. **Wording.** Do not use slang expressions, colloquialisms, vulgarisms, technical or trade terms, unless in a direct quote. Have the interviewee explain any technical concepts in non-technical language.

E-4. **Identifying persons.** Identify all persons mentioned in an investigative report to the fullest extent possible. The data listed below is in a vertical format, but you list it horizontally in all investigative reports. Semicolons will separate major areas and commas will separate elements within an area. Table E-1 (page E-2) shows the breakout for describing personal data.

Table E-1. Personal data

Major areas	*Format*
NAME:	Last, First, Middle (CI incident report)/First, Middle, Last (IMFR)
RANK/TITLE:	PFC, SFC, 1LT, MAJ, GS-12, WG-7
COMPONENT: (Block 7 of the Sworn Statement only)	RA, USAR, NG, Army Civilian, CIV, CON
SSN:	123-45-6789
DPOB: If Place is Unknown: If Date is Unknown:	DPOB: 9 July 1963, Indio, Iowa DOB: 9 July 1963/July 1963 POB: Indio, IA
DUTY POSITION:	Security Specialist (If unknown, list MOS)
DUTY LOCATION:	S-2, HQ, 503d MP Bn, 10th MP Bde, Fort Huachuca, AZ 85613
UNIT OF ASSIGNMENT:	HHC, 503d MP Bn, Fort Huachuca, AZ
RESIDENCE:	Room 8, Bldg 62702, HHC, 503d MP Bn Barracks, Fort Huachuca, AZ
PCS OR DEROS:	PCS: 29 March 2007/DEROS: 29 March 2007
TEMPORARY DUTY: (Do not list—for information purposes only.)	Upcoming dates and locations
ETS:	ETS: 25 July 2009/Indefinite
SECURITY CLEARANCE:	TOP SECRET/SECRET/NONE
LEVEL OF DAILY ACCESS TO CLASSIFIED INFORMATION:	TOP SECRET/SECRET/CONFIDENTIAL/NONE
SPECIAL ACCESS:	SCI (List only if applicable.)

1LT—first lieutenant
Bde—brigade
Bn—battalion
DEROS—date of return from overseas
DOB—date of birth
DPOB—date and place of birth
ETS—expiration term of service
GS—general schedule
HHC—headquarters and headquarters company
HQ—headquarters
IMFR—investigative memorandum for record
MAJ—major
MOS—military occupational specialty
MP—military police
NG—National Guard
PCS—permanent change of station
PFC—private first class
POB—place of birth
RA—Regular Army
SCI—sensitive compartmented information
SFC—sergeant first class
SSN—social security number
USAR—U.S. Army Reserve
WG—wage grade

Note 1. Write all security clearance information in capital letters.

Note 2. If source does not know a piece of information, do not list. Never address information as being unknown.

Jones, Robert Lee; SFC; SSN: 123-45-6789; DPOB: 9 July 1963, Indio, Iowa; Security Specialist, S-2, HQ, 503d MP Bn, 10th MP Bde, FH, Arizona; assigned to HHC, 503d MP Bn, FH; residing at Rm 8, Bldg 62702, HHC, 503d MP Barracks, FH; PCS: 29 March 2007; ETS: Indefinite; Security Clearance: TS, with daily access to TS.

E-5. **Qualifiers for names of persons:**

- **First name unknown (FNU).** If source does not know the first name of an individual, use the acronym "FNU." This acronym is always capitalized, used in its abbreviated form, and is never placed in parentheses. When using the term "FNU," or when the first name can be either male or female, ensure you indicate the gender of the individual. This may be through the use of an honorific title (Mr., Miss, Mrs., Ms., Dr.), a gender-specific pronoun (he, she), a specific reference to the gender (FNU Smith, a male,) or by other means that leave no doubt as to the gender of the individual. If the honorific title is used, place a period after the title (Mr., Mrs., Ms., Dr.).

CI incident report: Smith, FNU, a male	Smith, Mr. FNU
IMFR: FNU Smith, a male	Mr. FNU Smith

- **Middle name unknown (MNU).** If source does not know the middle name of an individual, the acronym "MNU" is used. If source knows the middle initial, do not use the acronym "MNU." In such cases, use the middle initial by itself followed by a period. This acronym is always capitalized, used in its abbreviated form, and is never placed in parentheses.

CI incident report: Smith, John MNU	Smith, John J.
IMFR: Jane MNU Jones	Jane M. Jones

- **Last name unknown (LNU).** If source does not know the last name of an individual, the acronym "LNU" is used. This acronym is always capitalized, used in its abbreviated form, and is never placed in parentheses.

CI incident report: LNU, John
IMFR: Jane LNU

Note. Do not use more than one personal name qualifier (FNU, MNU, LNU) in combination for the same person. In most cases, if you know only one of the components of the name (for example, only the first or last) simply omit MNU (for example, John LNU; or FNU Jones). Refer to an individual characterized as FNU, MNU, LNU, as an "Unidentified Individual."

- **No middle name (NMN).** If source knows an individual has no middle name, use (NMN). Always capitalize this acronym, use in its abbreviated form, and place in parentheses.

CI incident report: Smith, Jane (NMN)
IMFR: John (NMN) Jones

- **Initial only (IO).** When source knows that an individual's middle name is an initial only, the acronym "(IO)" is used. Always capitalize the acronym "(IO)," use it in its abbreviated form, and place it in parentheses after the initial.

CI incident report: Truman, Harry S (IO)
IMFR: Harry S (IO) Truman

- **Nicknames or alias.** If source identifies a person by a nickname or alias, place it in quotation marks.

Jones, John "Bubba"

E-6. **Military ranks and civilian titles.** When using a military rank as part of a person's title, or when listing a person's rank during initial identification in a CI report, express the rank using the standard Service abbreviation (see table E-2 [page E-4]). When referring to ranks and civilian titles or as part of a duty description, spell the rank out completely.

Table E-2. Military ranks and civilian titles

U.S. Army ranks	*Other Service ranks*	*Civilian titles*
PVT, PV2, PFC, SPC, CPL, SGT, SSG, SFC, MSG, 1SG, SGM, CSM, WO1, CW2, CW3, CW4, CW5, 2LT, 1LT, CPT, MAJ, LTC, COL, BG, MG, LTG, GEN. ***Note.*** Do not use periods with rank abbreviations.	Use the appropriate Service abbreviation and include the standard abbreviation for the Service, for example, MSgt/USAF, LtJG/USN, GySgt/USMC.	• For DOD civilians, use the appropriate civilian designation (for example, DAC for Army Civilians; DAFC for Air Force Civilians). • The combination of a civilian grade (for example, WG-5, WG-7, GS-12, GG-13, SES1, SES3) with a DOD civilian designation looks like—GG-13/DAC, WG-5/DAC, GS-12/DAFC. • For contract civilians, use the abbreviation CON. • For all non-DOD affiliated civilians, use CIV.
1, 2LT—first, second lieutenant 1SG—first sergeant BG—brigadier general CIV—civilian COL—colonel CON—contractor CPL—corporal CPT—captain CSM—command sergeant major CW2,3,4,5—chief warrant officer, W-2, 3, 4, 5 DAC—Department of the Army civilian DAFC—Department of the Air Force civilian	DOD—Department of Defense GEN—general GG—general schedule, excepted service GS—general schedule, competitive service GySgt—gunnery sergeant LTC—lieutenant colonel LTG—lieutenant general LtJG—lieutenant junior grade MAJ—major MG—major general MSG——master sergeant MSgt—master sergeant	PFC—private first class PV2—private, E-2PVT—private SES—Senior Executive Service SFC—sergeant first class SGM—sergeant major SGT—sergeant SPC—specialist SSG—staff sergeant USAF—U.S. Air Force USMC—U.S. Marine Corps USN—U.S. Navy WG—wage grade WO—warrant officer

E-7. **Physical descriptions.** If the name, with a unit of assignment or place of duty, is unknown, obtain and report the physical description of the individual. The data below is in a vertical format, but in all reports, list the information horizontally with semicolons separating major areas and commas separating the elements within an area. Table E-3 shows the breakout for describing physical descriptions.

Table E-3. Physical description

Major areas	*Format*
SEX:	Male, Female
RACE:	Caucasian, Black, Asian
SKIN COLOR:	Dark, Tan, White
SKIN COMPLEXION:	Smooth, Pock-marked
AGE:	Within a five-year range
HEIGHT:	Within a two-inch range
WEIGHT:	Within a ten-pound range
BUILD/POSTURE:	Small, Medium and stooped
HAIR:	Black, Brown, Gray, Blonde, Red, Bald
EYES:	Black, Brown, Blue Gray, Green
DRESS:	Headwear, upper to lower body wear, footwear, jewelry (top to bottom).
DISTINGUISHING CHARACTERISTICS:	Physical handicap, tattoos, body piercing, scars, birthmarks, moles (If no distinguishing characteristics, put “None.”)

Note. If your source does not know an item, do not list. Never address an item as being unknown.

SUBJECT: SEX: Male; RACE: Caucasian; SKIN COLOR: WHITE; SKIN COMPLEXION: Fair complexion; AGE: 35-40; HEIGHT: 5' 8"-5' 10"; WEIGHT: 165-175 pounds; BUILD: Medium; HAIR: Brown, to the top of the collar; EYES: Brown; DRESS: Blue, short sleeve polo shirt, blue jeans, white tennis shoes; DISTINGUISHING CHARACTERISTICS: Mole above the left eye; NFI.

E-8. **Referring to SUBJECT:**

- Always refer to a subject of an investigation, once initially identified, as SUBJECT. Always write the term "SUBJECT" in capital letters. The term "SUBJECT" replaces the surname, thus the article "the" never precedes the term.
- When using any pronoun in place of SUBJECT, write the pronoun in capital letters (for example, HE, SHE, HIS, HER).
- When there is more than one SUBJECT, identify each by placing a number after the word SUBJECT (for example, SUBJECT 1 and SUBJECT 2). Number subjects sequentially as they appear in the report. List subjects in the following order: Military personnel subject to the UCMJ, known U.S. persons, any known persons, and any unidentified persons. There are two ways to address multiple subjects. The first is "SUBJECT 1 and SUBJECT 2." The second is "SUBJECT 1 and 2." Either way is acceptable; however, you must be consistent throughout the report.
- When using any plural pronouns to refer to two or more subjects, the pronoun will be written in capitalized letters (for example, THEY, THEIR); when using a plural pronoun referring to a SUBJECT and another person, the pronoun will be written using normal capitalization (for example, they, their).

  SUBJECT 1 and SUBJECT 2 walked to THEIR car.
  Jones first met SUBJECT when they attended the Officer Basic Course.

- In CI reports, always write SUBJECT's surname with capital letters.

E-9. **Referring to source.** A source is always the person who provides the information in the report. For the CI incident report, the source is the Walk-in; for subsequent IMFR, the person interviewed is the source.

- Refer to the source of the investigation, once initially identified, by their surname in the CI incident report, but as source in the IMFR.

  CI incident report: Jones entered the vehicle.
  IMFR: Source entered the vehicle.

- When you refer to an individual as source in the IMFR, always write the word source in title case. The term "source" replaces source's surname in the IMFR, thus the article "the" never precedes the term in a report.
- When using any pronoun in place of source, the pronoun is always in title case (He, She, His, Her).
- Since source provided all the information contained in the report, do not state in the body of the report "Source said…" unless source is relating something He/She said to another person involved. Otherwise, if the information is contained in the report, it is implied source told the CI special agent the information.
- If source provides an opinion, you must identify it as such and provide a reason for the formulation of the opinion.

CI incident report: Smith believed SUBJECT did not like HIS commander because HE consistently made statements.

against him.
IMFR: Source believed SUBJECT did not like HIS commander because HE consistently made statements against him.

E-10. **Referring to other people.** When referring to any person in a report other than source or SUBJECT, address them by their surname and use lower case pronouns.

Source saw Jackson sitting at the bar by himself.

E-11. **Referring to source, SUBJECT, and other people in the same sentence.** When referring to source, SUBJECT, and other people in the same sentence, place source first, then follow with SUBJECT, and then all other people. Maintain this order no matter what combination of the above is involved.

Source, SUBJECT, and Jackson left the store together.
Source and Jackson left the bar together.
SUBJECT and Jackson drove away in the black car.

E-12. **Qualifiers.** These are abbreviations used to inform the reader that you asked additional developmental and clarifying questions, but source did not know the answer. Do not use these as a crutch for failing to fully develop all required information during an interview.

E-13. **Not further identified (NFI).** This qualifier applies to all persons, except source, identified in paragraph 4 of the CI incident report or paragraph 1 of the IMFR. Use this when source does not know complete identifying information concerning an individual. If you do not know at least one element of required identifying data, then use the term "Not Further Identified." Completely spell out the phrase "Not Further Identified" the first time it is used and follow it with its short title in parentheses (for example, Not Further Identified [NFI]) if you will use it again. Thereafter, only the short title "NFI" is used. Regardless of the way you write it, you must be consistent. Whenever using "NFI," whether spelled out or short-titled, you will precede it with a semicolon.

1SG Jones, First Sergeant, B Co, 309th MI Bn; NFI.

Note. Never use the term "NFI" for source since source will always know their identifying data. If source refuses to provide personal data, indicate the refusal in your report as the last entry in source's personal data block (for example, source refused to provide His SSN).

E-14. **Qualifying statement.** Enter a qualifying statement when a significant change of time, a location, or event occurs. Only use these statements when the source cannot provide specific details concerning significant details concerning the incident or SUBJECT of the investigation which Army Theater Counterintelligence Coordinating Authority (ATCICA), Army Counterintelligence Coordinating Authority (ACICA), or staff judge advocate (SJA) personnel would want to know to better guide the investigative process.

Jones (CI incident report) or source (IMFR) could provide no further pertinent information concerning SUBJECT 1's travel to Mexico to meet SUBJECT 2.

E-15. **Quotations.** Only use direct quotes if the exact wording is necessary for the reader to gain a complete understanding of what someone said or to emphasize the importance of the statement (for example, threats, confessions, direct statements). Place quotes in quotation marks and transcribe them verbatim. However, if source said "didn't" and the CI special agent writes "do not," the content of the statement did not change and will be acceptable. Do not use abbreviations or short titles in quotes unless the person quoted used them. If you must add your own parenthetical comments to a quote, place them in brackets, not parentheses. Brackets indicate an editorial comment from the agent. Place other items (for example, slang terms; colloquialisms; technical terms or military jargon; nicknames) in quotation marks as well.

SUBJECT 1 told SUBJECT 2, "I am going to the SCI."

E-16. **Numerals.** In general, spell out numbers from one to ten and write numbers above ten as a number. Exceptions to this rule are as follows:

- Use numerals, when associated with money.

$.05 (U.S.)
$5 (U.S.)
1,200 dinar (Iraq)
10,000 lira (Italian)
1,000 won (South Korea)

Note. Always identify the currency in lower case letters (not used for U.S. currency) and the country (use this for U.S. currency), in parentheses, associated with the currency.

- Use numerals when part of an address.

Room 5, Building 62702, Headquarters and Headquarters Company, 309th MI Bn Barracks, Fort Huachuca, AZ
Apartment 3, 766 North 7th Street, Sierra Vista, AZ

- Use numerals when expressing weights and measures.

5 pounds
3 feet
2 inches
1 kilometer
45 degrees Celsius

- Use numerals when expressing dates and times: Always use the 24-hour clock when expressing time. Do not follow the time with the word hours. If the date is a single digit, do not place a "0" in front. If source cannot provide an exact date, list what you have and follow up with "exact" date unknown."

At approximately 2245, 10 January 2008…
At approximately 0730, 1 January 2008…
In early March 2008, exact date unknown…

- Use numerals when identifying military units below corps. For a corps level unit, use Roman numerals.

Below Corps: B Company, 309th MI Bn, 111th MI Bde, Fort Huachuca
Corps Level: Headquarters, V Corps

- Spell out armies.

Third Army

- Use numerals when identifying telephone numbers, license plate numbers, and other numbers typically expressed by a number.

(520) 551-1212
AZ license plate number: ALO55Y
SSN: 012-34-5678

- Use numerals when expressing a percent. You will always spell out the word percent following the number.

5 percent
20 percent

- Use numerals when expressing a fraction that is part of a mixed-number; otherwise, spell out the fraction. If you use a fraction with other numbers, you will use the fraction. When describing an item which combines spelled-out numbers and numbers in written form, you will write out all numbers.

8 1/2
12 2/3
three-fifths
one-half
8 1/2 inches tall by 1/2 inch thick
8 cars and 15 trucks

- Avoid beginning a sentence with a number. It is often easy to reword a sentence to avoid this. If you cannot avoid beginning a sentence with a number, spell out the number.

WRONG: 15 minutes later, SUBJECT left.
RIGHT: Fifteen minutes later, SUBJECT left.
BETTER: SUBJECT left 15 minutes later.
BEST: At approximately (time), SUBJECT left.

E-17. **Unknown spelling of a word.** Spell out phonetically words whose spellings are unknown to either the CI special agent or source, with the word "phonetic" placed in parentheses immediately after the spelling. You do not need to put the word (phonetic) after subsequent uses of the name or word.

John MNU Sipowitz (phonetic)

E-18. **Foreign words.** Whenever you use a foreign word in a CI report, the foreign word will be underlined every time it is used. You will exclude surnames, company or organization names, and the names of foreign cities from this rule. If you know the English translation, place it in parentheses immediately following the foreign word the first time it is used.

Paregam (friend)
SUBJECT met Gomez at the Tankaran (museum).

E-19. **Underlining.** You will underline titles of publications, plays, magazines, web addresses, or titles of ships and you will include them exactly as written (regardless of whether words or phrases were previously abbreviated or short-titled).

SUBJECT carried a copy of <u>The Catcher in the Rye</u>, the book by author J.D. Salinger.
SUBJECT accessed <u>www.us.army.mil</u> on a daily basis.
While assigned to the S3, HQ, 309th MI Bn, SUBJECT obtained a copy of the document entitled <u>111th Military Intelligence Brigade General Defense Plan 06-01</u> (U), classified SECRET, dated 3 February 2008

Note. Do not underline the classification of a document title unless it is part of the title (see third example above).

E-20. **Contractions.** Do not use contractions in CI reports. The only exception is if the contraction is part of a direct quote or the title of a publication.

Correct:	cannot, they are, did not
Incorrect:	can't, they're, didn't

E-21. **Abbreviations.**

- Abbreviate words having commonly used military abbreviations if used more than once in the report. Completely spell out the word the first time it is used, and place the abbreviation in parentheses immediately following the word. Thereafter, use only the abbreviation (without the parentheses).

Department of the Army (DA) Form 2823 DA Form 3881 Army Regulation (AR) 381-10 AR 381-20

- Do not abbreviate the names of foreign countries. Spell out the country name in full the first time it is mentioned. Thereafter, use the two-letter DI country code.

Seoul, Republic of South Korea Taegu, KS

- Do not abbreviate military ranks when used as a duty position or when referring to the rank in general terms (for example, not as part of a person's title).

SFC John Smith is assigned to B Co, 309th MI Bn. He is a Platoon Sergeant in B Co, 309th MI Bn.

- Abbreviate civilian titles preceding surnames. Abbreviations for junior (Jr.) and senior (Sr.) will be abbreviated when used as part of the name. A period will follow both titles and name designators.

Dr. John Smith John Smith Sr.

- Do not abbreviate months or years. Completely spell out months, and years will always contain all four digits.

9 July 1963 10 October 2008

- U.S. is the only authorized abbreviation that does not have to be spelled out before its subsequent use. Write US without periods. Use this in all reports and the sworn statement.

E-22. **Short titles.** Short titles are similar to abbreviations, but you use them for titles (such as military branches, organizations). As with abbreviations, you use them only if you use the word to be short-titled more than once in the report. To form a short title, completely spell out the title the first time it is used. Take the first letter of each proper noun in the title (do not use the first letters of articles and prepositions in the short title) and place the short title in parentheses after the title. Thereafter, use only the short title without the parentheses. Short titles are not required in a report; however, whether abbreviated or not, consistency throughout the report is required.

First time used: Headquarters and Headquarters Company (HHC) Subsequent use: HHC

Note 1. Do not use short titles if the short title might be confused with a commonly used short title or abbreviation. For example, if you use Michigan/MI for several addresses, and then mention Michigan later in your narrative, you cannot use MI in the sentence because MI is normally military intelligence; the same applies for Fort Lewis (FL); FL is the postal abbreviation for Florida.

Note 2. Try to avoid using short titles at any time on the Sworn Statement (DA Form 2823), unless part of a quote or title.

E-23. **U.S. states.** When referencing to U.S. states, spell out the state completely the first time it is used. Thereafter, use only the two-letter U.S. Postal Service abbreviation. Do not place the postal abbreviation in parentheses after spelling out the state. This is because the postal abbreviations are commonly accepted abbreviations. After a state is mentioned in the report, abbreviate the state when referred to alone. If a city is mentioned a second time, the state does not have to be placed after. If a new city is mentioned in the state, then the postal abbreviation is used.

First time used: Sierra Vista, Arizona Second time used: Sierra Vista New city: Tucson, AZ Second time used: Tucson

E-24. **Smallest to largest rule.** Whenever referring to items with multiple components, list the smallest component first in succession to the largest component.

Times/Dates: Time/Day/Month/Year (At 0900, 12 February 2005) Addresses: House number, street, city, state or country (123 Main Street, Sierra Vista, Arizona) Military units: Company, Battalion, Brigade, Installation, State/Country

E-25. **Lowest common denominator.** The lowest common denominator technique is a method of expressing multiple elements of the same larger element without redundancy. For example, in a single report, there may be multiple companies mentioned that all belong to the same battalion. Applying the lowest common denominator rule, we need only identify subsequent elements up to the point that they share a common element (lowest common denominator) with a previously fully identified element. As a rule, at least two elements must be included, and the lowest common denominator must be unique. Thus, B company cannot be a lowest common denominator because there are many B companies in the Army; however, 309th MI Battalion is the lowest common denominator because there is only one 309th MI Battalion in the Army. The lowest common denominator technique is not required; however, whether used or not, consistency throughout the report is required.

First time identified: B Company (Co), 309th Military Intelligence (MI) Battalion (Bn), 111th MI Brigade (Bde), Fort Huachuca (FH), Arizona. Subsequent mention of first unit: B Co, 309th MI Bn. Different unit identified: D Co, 309th MI Bn, FH. Subsequent mention of unit: D Co, 309th MI Bn.

COUNTERINTELLIGENCE INCIDENT REPORT

E-26. All CI incident reports will be prepared in the prescribed format written in Arial font, font size 12. Specific examples for CI incident reports are provided in this section. The following is a step-by-step explanation of the format shown in figure E-1 (page E-16).

E-27. **Overall classification.** The overall classification will be marked on the top and bottom of each page in bold. The font for this will be Arial font, font size 14. You will classify your reports based on the CI category, and will at a minimum be classified CONFIDENTIAL.

UNCLASSIFIED CONFIDENTIAL SECRET TOP SECRET

E-28. **Portion markings.** Each paragraph will be marked with the appropriate portion marking placed in parentheses at the beginning of the paragraph between the paragraph number and the beginning of the text. The portion markings will have two spaces before and two spaces after the parentheses.

4. (U) PERSONS INVOLVED:
a. (X//XX) SUBJECT: SMITH, John A.; SSG…

4. (U) PERSONS INVOLVED:
a. (U) SUBJECTS:

1. (X//XX) SUBJECT 1: SMITH, John A.;…
2. (X//XX) SUBJECT 2: JONES, John B.;…

E-29. **Classification/Declassification authority.** These will appear on the bottom left hand side of the first page, two spaces from last line of text. For all reports, classification authority and declassification instructions are as follows:

DERIVED FROM: Sec 2-2, Chapter 2
INSCOM SCG 380-2
DECLASSIFY ON: X1
DATE OF SOURCE: 6 Dec 96

E-30. **Heading, office symbol, and date.** All reports will begin with appropriate DA letterhead, office symbol, and date.

DEPARTMENT OF THE ARMY
307th MILITARY INTELLIGENCE BATTALION
902d MILITARY INTELLIGENCE GROUP
FORT HUACHUCA, ARIZONA 85613

ATZS-TPQ-A (report date)

E-31. **Memorandum for.** Triple space the MEMORANDUM FOR line below the office symbol. For training purposes, list it as follows:

MEMORANDUM FOR
ARMY CI COORDINATING AUTHORITY, ATTN: DAMI-CH-CCO, FORT MEADE, MD 20755-5955
COMMANDER, 902D MI GROUP, ATTN: IAMG-OP-ATCICA, FORT MEADE, MD 20755-5955
COMMANDER, FOREIGN CI ACTIVITY, ATTN: IAFC-FCA, FORT MEADE, MD 20755-5955

E-32. **Subject block.** Double spaced below the last address in the MEMORANDUM FOR line is the subject block. This block is a four-line entry which you may write, depending on the information known, as a personal or impersonal subject block.

E-33. **Personal subject block.** You will use Line 1 when there is only one SUBJECT and you know the identity of SUBJECT. This incorporates last name, first name, and middle initial (if known). Line 2 will contain the rank and SSN (if known). If you know the identity of SUBJECT, but you are missing some of the information needed for inclusion in the subject title, report the information known (for example, CIV, ARMY). Line 3 will contain the DPOB. If you know the identity of SUBJECT, but information needed for inclusion is incomplete, you will list the known information. The classification covering the first three lines will follow. The classification will normally be CONFIDENTIAL. Line 4 will contain the local case control number (LCCN). The format for the LCCN will list the field element brevity code, the last two numbers of the fiscal year, and the sequence number. The classification for line 4 will always be UNCLASSIFIED and represented by a "(U)."

SUBJECT: SMITH, John J.
2LT; 123-45-6789
9 July 1963, Sierra Vista, Arizona (X//XX)
LCCN: TFO-06-005 (U)

SUBJECT: SMITH, John
U.S. ARMY
1963, Arizona (X//XX)
LCCN: TFO-06-005 (U)

E-34. **Impersonal subject block.** You will use Line 1 when the identity of SUBJECT is unknown or when there is more than one SUBJECT. This incorporates the city and state where the incident took place. Line 2 will consist of the appropriate CI Investigative Case Category. Line 3 will contain the date of incident as specific as possible (for example, 1 January 2008); if source reports dates in a sequential order (for example, 14-16 January 2008), you will list them as such. If multiple dates are given, but are not in a sequential order, the student will use the earliest date. The classification of the first three lines will follow. The classification will normally be CONFIDENTIAL. Line 4 will contain the LCCN. The format for the LCCN will list the field element brevity code, the last two numbers of the fiscal year, and the sequence number. The classification for line 4 will always be UNCLASSIFIED and represented by a "(U)."

SUBJECT: Fort Huachuca, Arizona
Espionage
9 July 2008 (X//XX)
LCCN: TFO-06-005 (U)

SUBJECT: Fort Huachuca, Arizona
Espionage
14-16 January 2008 (X//XX)
LCCN: TFO-06-005 (U)

E-35. **Paragraph 1 (SUMMARY).** The summary must be clearly written to show an incident within CI jurisdiction occurred and the significance of that incident. The summary should answer the six interrogatives. You will address all U.S. military persons involved by service, rank, and unit (lowest common denominator) (for example, An Army Staff Sergeant assigned to the 309th MI Battalion). You will address foreign military members by their nationality, component, and rank (for example, A Republic of South Korea Navy Captain). Address Army Civilians as such (for example, A Department of the Army Civilian). You will address all other civilians by nationality and title or status (for example, A U.S. Contractor; a Republic of South Korea Local Hire Employee; or an unidentified foreign national). Items such as a title of a classified document may be nice-to-know information, but you may refer to them generically due to space constraints. The summary of information (SOI) can exceed five lines but should not be a paragraph that takes up half the page. If you use short titles in the report, then you may start them in this paragraph. If you do not start short titles in this paragraph, they will start in paragraph 3. The summary paragraph should also include the Army command and technology involved in the incident.

1. (X//XX) SUMMARY: An Army Staff Sergeant at the 309th Military Intelligence (MI) Battalion (Bn) reported that He observed a U.S. Army Lieutenant Colonel assigned to the 309th MI Bn make unauthorized copies of a classified document, place them in HIS battle dress uniform and leave the sensitive compartmented information facility (SCIF). A U.S. Army Major assigned to the 309th MI Bn was present and may have observed the incident. Army Command: TRADOC; Technology Involved: Unknown.

E-36. **Paragraph 2 (DATE OF INCIDENT).** This date must always match the date provided in line 3 of the subject block. If the incident consists of a time period, then the entire period is shown here. The subject block will have only the earliest date. See subject block examples for examples of how to list the date of incident. This will only apply when using an impersonal subject block.

E-37. **Paragraph 3 (LOCATION OF INCIDENT).** This is the complete address where the incident took place. In a city, this will include the number, street, city, and state. On a military installation, this will include room, building, unit, installation, and state. When using an impersonal subject block, the location in line 1 of the subject block will contain the city and state or city and country for OCONUS of the incident. If elements of the location are missing, use the statement: "Source could provide no further pertinent information concerning the location."

2. (X//XX) LOCATION OF INCIDENT: Building (Bldg) 2587, Headquarters (HQ), 309th Military Battalion, Fort Huachuca, Arizona. Source could provide no further pertinent information concerning the location.
3. (X/XX) LOCATION OF INCIDENT: City Lights Restaurant, 1234 Pratt Street, Baltimore, Maryland.

E-38. **Paragraph 4 (PERSONS INVOLVED).** Provide all known identifying data for SUBJECT(S), source, Witness(es), and Others Knowledgeable, in that order. If you do not have a name and unit of assignment or duty location on an individual, include a physical description in narrative format. When you report personal data or physical descriptions, include only known information. If source told you SUBJECT has no security clearance, you just received a positive response. You would list security clearance in the identifying data and follow it with the word "NONE." If source told you they do not know the individual's security clearance, you did not receive a positive response. You will omit the security clearance information from the identifying data paragraph.

4. (U) PERSONS INVOLVED:

a. (X//XX) SUBJECT (S):

(1) (X//XX) SUBJECT 1: MILLER, Susan Lynn; LTC; SSN: 111-22-3333; DPOB: 23 June 1965, Shawmutt, Pennsylvania; Commander, 309th Military Intelligence (MI) Battalion (Bn), Fort Huachuca (FH), Arizona; ETS: Indefinite; Security Clearance: TOP SECRET, with access to NONE; Not Further Identified (NFI).

(2) (X//XX) SUBJECT 2: GENDER: Male; RACE: Caucasian; SKIN COLOR: Tan; SKIN COMPLEXION: Smooth; AGE: 35 - 40; HEIGHT: 5' 8" - 5' 10"; WEIGHT: 165 - 175 pounds; BUILD: Medium; HAIR: Brown, to the top of the collar; EYES: Brown; DRESS: Blue short, sleeve polo shirt, blue jeans, white tennis shoes; DISTINGUISHING CHARACTERISTICS: Mole above the left eye; NFI.

E-39. **Privacy Act Caveat.** Before the start of paragraph 5, the appropriate Privacy Act Caveat is listed three spaces below the subject block, three spaces above paragraph 5, and centered.

E-40. **Paragraph 5 (NARRATIVE).** Paragraph 5 is the incident information as told by source. Paragraph 5a starts the incident information. Use as many subparagraphs as necessary to relay the incident information. Generally, short subparagraphs are easier to read than long ones. Remember, in formal writing, a paragraph consists of no more than 10 lines of text.

AUSTIN HAD NO OBJECTION TO HIS IDENTITY BEING RELEASED

5. (U) NARRATIVE:

a. (X//XX) On 15 August 2005, Davis had dinner with Witnesses at Wagon Wheel, Sierra Vista, AZ. Davis and Witnesses generally go out to eat together once per week in the Sierra Vista area. Davis saw SUBJECT 1 on several occasions eating in various restaurants, but this was the first time Davis witnessed SUBJECT 1 meeting with SUBJECT 2.

E-41. **Period of association.** After fully listing the incident information, identify source's association with SUBJECT. List the information in the following order: the type of contact SUBJECT and source have (professional and social); when source first met SUBJECT and the circumstances of that meeting; and frequency of the contact. This will incorporate all periods of contact; if there are breaks in contact, address professional or social contact for each period. It is possible for source to have no period of association if source and SUBJECT have never met.

E-42. **Counterespionage (CE) indicators.** CE indicators are signs generally exhibited by persons committing a national security crime. The seven indicators are financial matters; personal conduct; loyalty and allegiance; outside activities; work habits; foreign considerations; or emotional, mental, or personality disorders. You will list the first CE Indicator exhibited by SUBJECT in the same subparagraph as the period of association. If you identify more than one CE Indicator, list each in a separate subparagraph, following the initial one listed in the period of association subparagraph.

E-43. Example of a known SUBJECT with known CE Indicators.

g. (X//XX) Source had daily professional and no social contact with SUBJECT since early November 2004, exact date not recalled, when He was assigned to HHC, 309th MI Bn. SUBJECT often complained to Austin about not earning enough money to meet HIS monthly obligations, but spent a lot of money when not at work. Source could provide no further pertinent information concerning SUBJECT's financial matters.

h. (X//XX) SUBJECT was often seen intoxicated outside HIS place of duty and 1SG Collins, B Co, 309th MI Bn, counseled SUBJECT on at least three occasions concerning HIS alcohol consumption. Source could provide no further pertinent information concerning SUBJECT's personal conduct.

i. (X//XX) Source could provide no pertinent information concerning SUBJECT's loyalty/allegiance, outside activities, work habits, foreign considerations, or emotional/mental/ personality disorders.

E-44. Example of a known SUBJECT with no known CE Indicators.

j. (X//XX) Source never met SUBJECT 1 before this incident and could provide no pertinent information concerning SUBJECT 1's financial matters, personal conduct, loyalty/allegiance, outside activities, work habits, foreign considerations, or emotional/mental/ personality disorders.

E-45. Example of an unknown SUBJECT with no known CE Indicators.

j. (X//XX) Source never saw SUBJECT 2 before this incident and could provide no pertinent information concerning SUBJECT 2's financial matters, personal conduct, loyalty/allegiance, outside activities, work habits, foreign considerations, or emotional/mental/ personality disorders.

E-46. **Motivation.** After you list the last CE Indicator, a separate subparagraph will list walk-in source's motivation for reporting the incident.

i. (X//XX) Henslee reported this incident due to Her concern over SUBJECT 1's lack of good security practices. It concerned Henslee that SUBJECT 2 asked if SUBJECT 1 worked at that location and then took the trash which would have contained the classified flash memory drive.

E-47. **Paragraph 6 (ACTIONS TAKEN).** This is the paragraph where you list all actions taken which fall under the standing investigative authority. These include, but are not limited to sketches, sworn statement, documents, records checks, and a Secrecy Affirmation Statement.

6. (U) ACTIONS TAKEN:

a. (U) Local agency checks (LACs)/military agency checks (MACs) initiated on all SUBJECTS to obtain full identifying data. Results will be reported via IMFR.

b. (U) Smith provided a sketch of the incident area.

c. (U) Smith read and signed a Nondisclosure Agreement and executed a Sworn Statement.

E-48. **Paragraph 7 (AGENT'S COMMENTS).** In this paragraph, you will write the Freedom of Information Act (FOIA), provide the CI Investigation Case category justification, and any comments that you, as the CI special agent, have.

7. (X//XX) AGENT"S COMMENTS: Agent names and any other personal identifying information are exempt from release under FOIA exemptions 6 and 7 (civilians: 5 USC §§ 552(b)(6) and (b)(7)(c)) and may not be disclosed in response to FOIA requests for intelligence information reports (IIRs) or other intelligence investigative documents. This office assesses this incident as a Security Matter (Loss) based on what appears to be the unauthorized removal of classified material from the sensitive compartmented information facility (SCIF), which SUBJECT 1 then passed to an unauthorized individual. Recommend ATCICA open an investigation to determine the circumstances surrounding SUBJECT 1's removal of classified material from the SCIF.

E-49. **Paragraph 8 (REPORT PREPARED BY).** This paragraph identifies the CI special agent who prepared the report, their unit, telephone numbers (defense switching network [DSN] and commercial), and fax numbers.

8. (U) REPORT PREPARED BY: David M. Jones, special agent, Fort Huachuca Field Office, 902d MI Group, SECURE TELEPHONE: DSN: 888-9203, COMMERCIAL: (623) 345-9203; SECURE Fax: DSN: 888-9204, COMMERCIAL: (623) 345-9204.

E-50. **Paragraph 9 (EXHIBITS).** In this paragraph, you will list all attachments to the report and the date you received the attachments. If the exhibit is not dated, list it as "undated." This includes, but is not limited to sworn statements, sketches, and documents. If there are any exhibits listed, you will place an

open set of parentheses before listing the exhibit. Investigating personnel will use the open parentheses to identify exhibits during the course of the investigation once ATCICA closes the case or transfers it to another agency. The parentheses will contain four spaces. The exhibit will then be listed two spaces after.

E-51. **Example of no exhibits.**

9. (U) EXHIBITS: NONE.

E-52. **Example of one exhibit.**

9. (U) EXHIBITS: ( ) DA Form 2823, Sworn Statement, executed by Jacobs, John J., dated 20 April 2008.

E-53. **Example of multiple exhibits.**

9. (U) EXHIBIT(S): a. (U) ( ) Sworn Statement, executed by Jacobs, John J., dated 20 April 2008. b. (X//XX) ( ) Sketch of incident area, executed by Jacobs, John J., dated 20 April 2008. c. (U) ( ) Computer diskette, updated.

E-54. **Signature block.** The signature block follows paragraph 9. Place the signature block five lines below the last line of text with the first letter centered on the page. It is mandatory that there are at least two lines of text before the signature block (for example, your signature block will not be the only thing on a page). Line 1 of the signature block is the CI special agent's name in capital letters. Line 2 consists of the words "special agent," and line 3 is the unit of assignment.

JUSTIN J. BLACK Special Agent A Co, 307th MI Bn

E-55. To the left of the signature block, type the word "EXHIBIT" (all caps) on the same line as the agent's name. Directly below EXHIBIT, type "as"; both words will be left justified.

E-56. Figure E-1 is an example of an CI incident report.

CLASSIFICATION

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

ATZS-TPQ-A 21 May 2008

MEMORANDUM FOR
ARMY CI COORDINATING AUTHORITY, ATTN: DAMI-CH-CCO, FORT MEADE, MARYLAND 20755
COMMANDER, 902D MILITARY INTELLIGENCE BRIGADE, ATTN: IAMG-OP-ATCICA, FORT MEADE, MARYLAND, 20755
COMMANDER, USAFCA, 902D MI GROUP, ATTN: IAFC-OP, FORT MEADE, MARYLAND 20755

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

1. (X//XX) SUMMARY: At approximately 1645, 19 May 2008, an Army Specialist assigned to 1st Signal Brigade (Bde), found a classified flash memory drive in a trashcan located at an Army Staff Sergeant's desk. An Army Sergeant assigned to the 1st Signal Bde, removed the flash memory drive from the trashcan, and secured it. At approximately 1730, an Unidentified Individual asked the Specialist if the Staff Sergeant worked in Building 52204. When the Specialist told the Unidentified Individual the Sergeant worked at the location, the Unidentified Individual took the trash out of the nearby trash dumpster and left the area. MACOM: TRADOC; Technology Involved: Unknown.

2. (U) DATE OF INCIDENT: 19 May 2008.

DERIVED FROM: Sec 2-2, Chapter 2, INSCOM SCG 380-2
DECLASSIFY ON: X1
DATE OF SOURCE: 6 Dec 96

CLASSIFICATION

Figure E-1. Example of a CI incident report

CLASSIFICATION

ATZS-TPQ-A 21 May 2008

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

3. (X//XX) LOCATION OF INCIDENT: Building 52204, Headquarters (HQ), 1st Signal Bde, Fort Huachuca (FH), Arizona.

4. (U) PERSONS INVOLVED:

a. (X//XX) SUBJECT (S):

(1) (X//XX) SUBJECT 1: RIVERA, Brenda MNU; SSG; DPOB: 12 March 1976, Pittsburgh, Pennsylvania; Plans Noncommissioned Officer, S3, HQ, 1st Signal Brigade; assigned to Headquarters and Headquarters Company (HHC), 1st Signal Bde, FH; Residence: Apartment 105, Mountain View Apartment Complex, 800 Carmichael Street, Sierra Vista, AZ; Security Clearance: TOP SECRET, with access to SECRET; Special access: SENSITIVE COMPARTMENTED INFORMATION; Not Further Identified (NFI).

(2) (X//XX) SUBJECT 2: SEX: Male; RACE: Hispanic; SKIN COLOR: Light Tan; SKIN COMPLEXION: Clear Complexion; AGE: 30-35; HEIGHT: 5'11"-6'1"; WEIGHT: 160-170 pounds; BUILD: Medium; HAIR: Brown; EYES: Brown; DRESS: Beige short sleeve shirt with a Cochise Disposal Systems (CDS) logo, beige khaki pants; DISTINGUISHING CHARACTERISTICS: None; NFI.

b. (X//XX) SOURCE: Henslee, Jane Brittany; SPC; SSN: 123-45-6789; DPOB: 3 July 1984; San Jose, California; Administrative Specialist, S3, Room 5, Building 52204, HQ, 1st Signal Bde; assigned to HHC, 1st Signal Bde; Residence: Room 238, Building 52106, HHC, 1st Bde Barracks, FH; ETS: 29 August 2009; PCS: 20 March 2007; Security Clearance: SECRET, with daily access to SECRET; Special access: NONE.

CLASSIFICATION

Figure E-1. Example of a CI incident report (continued)

CLASSIFICATION

ATZS-TPQ-A 21 May 2008

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

c. (X//XX) WITNESS: Carr, David MNU; SGT; POB: Billings, Montana; Transportation Sergeant, S3, Room 11, Building 52204, HQ, 1st Signal Bde, FH; assigned to HHC, 1st Signal Brigade; ETS: Indefinite; Security Clearance: TOP SECRET; with daily access to TOP SECRET; Special access: NONE; NFI.

d. (U) OTHERS KNOWLEDGEABLE: UNKNOWN.

5. (X//XX) NARRATIVE:

HENSLEE HAD NO OBJECTION TO HER IDENTITY BEING RELEASED

a. (X//XX) At approximately 1630, 19 May 2008, Henslee and Carr started cleaning and conducting end-of-day security checks in the HQ, 1st Signal Bde. At approximately 1645, Henslee started to take the clear plastic bag from the trashcan located at the front right-hand corner of SUBJECT 1's desk, and noticed the trash can contained a classified flash memory drive. The title of the document contained in the flash memory drive, 1st Signal Brigade General Defense Plan 01-06(U), classified SECRET, with a NOT RELEASABLE TO FOREIGN NATIONALS handling caveat, was embroidered on a black cloth lanyard attached to the flash memory drive. Henslee called Carr, the detail supervisor, over to the trash can and showed him the flash memory drive. Carr removed the flash memory drive from SUBJECT 1's trash can and secured it in the HQ, 1st Signal Bde security container. The security container was a gray, five-drawer, Mosler, General Services Administration approved security container, accredited to store SECRET information. Henslee could provide no further pertinent information regarding the flash memory drive, the classified document or the security container.

b. (X//XX) After Carr removed the flash memory drive he told Henslee to look through the remaining trash to make sure there was no other classified information. Henslee told Carr She did not find any other classified materials. Henslee could provide no further pertinent information concerning the conversation.

CLASSIFICATION

Figure E-1. Example of a CI incident report (continued)

CLASSIFICATION

ATZS-TPQ-A 21 May 2008

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

c. (X//XX) Carr secured the flash memory drive, Henslee emptied the remaining trash cans, and at approximately 1700 She collected all the bags and took them out to the dumpster located in the parking lot behind Building 52204. The parking lot was approximately 100 meters northeast of Building 52204. The dumpster stood alone in the southwest portion of the parking lot, perpendicular to two rows of marked parking slots. The dumpster was blue, approximately 3' x 5', with a sloping top approximately 3 feet in the front and approximately 4 feet in height in the back. Henslee walked back to the HQ after She threw away the trash and helped Carr complete the clean up and end-of-day security checks. Henslee could provide no further pertinent information about the dumpster or its location.

d. (X//XX) Once Henslee and Carr finished the security checks, they departed the HQ, locked the building, and walked behind Building 52204 to a parking lot adjacent to the trash dumpster. Carr intended to give Henslee a ride in the HQ duty vehicle to the barracks, since She did not have a car. As Henslee approached the HQ vehicle, She noticed SUBJECT 2, approximately 75 feet away, looking through several trash bags that were on the ground in front of the dumpster. SUBJECT 2 loaded the trash bags into the back of a CDS vehicle. SUBJECT 2 walked towards Henslee. When HE came within 10-20 yards of Henslee and Carr, HE asked if SUBJECT 1 worked in Building 52204. Henslee told SUBJECT 2 SHE did. SUBJECT 2 turned around and returned to the area of the dumpster. SUBJECT 2 removed some trash bags from the dumpster and loaded them into the back of the CDS vehicle. Henslee and Carr entered the duty vehicle and Carr drove Henslee to the barracks. Henslee could provide no further pertinent information regarding SUBJECT 2, the CDS vehicle, the contents of the trash bags or the incident.

e. (X//XX) Henslee had daily professional contact with SUBJECT 1 since early March 2008, exact date not recalled, when She was assigned to HHC, 1st Signal Bde. Henslee had no social contact with SUBJECT 1. SUBJECT 1 complained about being overworked and not having enough money to pay HER bills. Henslee could provide no further pertinent information concerning SUBJECT 1's finances.

CLASSIFICATION

Figure E-1. Example of a CI incident report (continued)

CLASSIFICATION

ATZS-TPQ-A 21 May 2008

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

f. (X//XX) SUBJECT 1 did not accomplish HER projects, had a cluttered desk, and seemed to spend more time looking for paperwork than actually working. Henslee could provide no further pertinent information concerning SUBJECT 1's work habits.

g. (X//XX) Henslee could provide no pertinent information concerning SUBJECT 1's, personal conduct, loyalty/allegiance, outside activities, foreign considerations, or emotional/mental/ personality disorders.

h. (X//XX) Henslee never saw SUBJECT 2 before the incident and could provide no information concerning SUBJECT 2's financial matters, personal conduct, loyalty/allegiance, outside activities, work habits, foreign considerations, or emotional/mental/ personality disorders.

i. (X//XX) Henslee reported this incident due to Her concern over SUBJECT 1's lack of good security practices. It concerned Henslee that SUBJECT 2 asked if SUBJECT 1 worked at that location and then took the trash which would have contained the classified flash memory drive.

6. (U) ACTIONS TAKEN:

a. (U) LACs and MACs were initiated on SUBJECT 1, results will be reported via IMFR.

b. (X//XX) Henslee provided a hand-drawn sketch of the trash dumpster area.

c. (X//XX) Henslee read and signed a nondisclosure agreement and executed a DA Form 2823, Sworn Statement.

CLASSIFICATION

Figure E-1. Example of a CI incident report (continued)

CLASSIFICATION

ATZS-TPQ-A 21 May 2008

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

7. (X//XX) COMMENTS: Agent names and any other personal identifying information are exempt from release under FOIA Exemptions 6 and 7 (5 USC §§ 552(b)(6) and (b)(7)((c)), and may not be disclosed in response to FOIA requests for IIRs or other intelligence investigative documents. This office assesses this incident as a SM01, based on what appears to be the planned unauthorized transfer of classified material to unauthorized personnel. Recommend that ATCICA CONUS open an investigation to determine the circumstances surrounding SUBJECT 1's possible planned unauthorized transfer of classified information to SUBJECT 2.

8. (U) REPORT PREPARED BY: Justin J. Black, Special Agent, Alaska Field Office, A Co, 307th MI Bn, 902d MI Group, SECURE TELEPHONE: DSN: 888-9203, COMMERCIAL: (520) 533-9203; SECURE Fax: DSN: 533-9204, COMMERCIAL: (520) 533-9204.

9. (U) EXHIBITS:

a. (U) ( ) DA Form 2823, Sworn Statement, dated 20 May 2008.

b. (U) ( ) Sketch of incident area; executed by Henslee, Jane B., dated 20 May 2008.

EXHIBITS
as

JUSTIN J. BLACK
Special Agent
A Co, 307th MI Bn

CLASSIFICATION

Figure E-1. Example of a CI incident report (continued)

INVESTIGATIVE MEMORANDUM FOR RECORD

E-57. **IMFR format.** All IMFRs will be prepared in the prescribed format in Arial font, font size 12. This includes non-IMFR (for example, records checks), specific examples for records checks are provided in this section. The following is a step-by-step explanation of the format shown in figures E-2 through E-6 (pages E-24 through E-44).

E-58. **Overall classification.** The overall classification will be marked on the top and bottom of each page in bold. The font for this will be Arial/14. You will classify your reports based on the CI category.

UNCLASSIFIED
CONFIDENTIAL
SECRET
TOP SECRET

E-59. **Portion markings.** Each paragraph will be marked with the appropriate portion marking placed in parentheses at the beginning of the paragraph between the paragraph number and the beginning of the text. The portion markings will have two spaces before and two spaces after the parentheses.

E-60. **Classification/Declassification authority.** These will appear on the bottom of the first page, two spaces from last line of text. For all reports, classification authority and declassification instructions are as follows:

DERIVED FROM: Sec 2-2, Chapter 2
INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 6 Dec 96

E-61. **Heading, office symbol, and date.** All reports will begin with appropriate DA letterhead, office symbol, and date. For training purposes, enter the heading as follows:

DEPARTMENT OF THE ARMY
307th MILITARY INTELLIGENCE BATTALION
902d MILITARY INTELLIGENCE GROUP
FORT HUACHUCA, ARIZONA 85613

ATZS-TPQ-A (report date)

E-62. Place IMFR double spaced below the office symbol, or enter REPORT OF ACTIVITY as appropriate.

E-63. **Subject block.** Double spaced below the INVESTIGATIVE MEMORANDUM FOR RECORD line is the subject block. Once the CI special agent sends the CI incident report to the ATCICA, the ATCICA will send a message back indicating whether they will open the case or if the case does not fall within CI jurisdiction. If ATCICA opens the case, the message will provide the new subject block which investigative personnel will use throughout the rest of the investigation. Normally the first three lines will not change, however line four will. ATCICA will replace the LCCN with an ASCCN. The ASCCN will always be UNCLASSIFIED and represented by a "(U)."

SUBJECT: SMITH, John J.
2LT; 123-45-6789
9 July 1963, Sierra Vista, Arizona (X//XX)
ASCCN: 06-111-902 (U)

SUBJECT: SMITH, John
U.S. ARMY
1963, Arizona (X//XX)
ASCCN: 06-111-902 (U)

E-64. **Privacy Act Caveat.** Before the start of paragraph 1, the appropriate Privacy Act Caveat is listed three spaces below the subject block, three spaces above paragraph 1, and centered.

E-65. **Paragraph 1.** This paragraph contains, in this order, the date the interview was conducted; source's name (first, middle, last) with full identifying data; SUBJECT(S) names (first, middle, last) with full identifying data; and the reason for the interview. As with the CI incident report, all grammatical guidelines apply. Once you identify the person providing the information in paragraph 1, the word "source" will substitute for that person's surname.

1. (X//XX) On 1 October 2008, an interview of <source's full name; first, middle, last and identifying data>, hereinafter referred to as source, provided information concerning <SUBJECT 1's name and known personal data>; SUBJECT 1 and <SUBJECT 2's name and known personal data or description>; SUBJECT 2 of this investigation. The purpose of this interview was to determine what knowledge source had pertaining to the mishandling of classified information, and possible espionage activity concerning SUBJECT 1 and 2. Source provided the following information:

E-66. **Paragraph 1a.** This sub-paragraph starts the incident information. Use the same format as paragraph 5 of the CI incident report.

E-67. The last sub-paragraph of paragraph 1 will list all actions taken. These include, but are not limited to sketches, sworn statement, documents, records checks, and a Secrecy Affirmation Statement.

E-68. **Paragraph 2 (AGENT'S COMMENTS).** In this paragraph, you will write the Freedom of Information Act and any comments that you, the CI special agent, have.

2. (X//XX) AGENT'S COMMENTS: Agent names and any other personal identifying information are exempt from release under FOIA exemptions 6 and 7 (civilians: 5 USC §§ 552(b)(6) and (b)(7)(c)) and may not be disclosed in response to FOIA requests for IIRs or other intelligence investigative documents.

E-69. **Exhibits.** Exhibits are listed to the left of the signature block (left justified).

E-70. Example of no exhibits:

Exhibits None	VINCENT K. MCMAHON Special Agent A Co, 307th MI Bn

E-71. Example of one exhibit:

Exhibits ( ) DA Form 2823	VINCENT K. MCMAHON Special Agent A Co, 307th MI Bn

E-72. Example of multiple exhibits:

Exhibits ( ) DA Form 2823 ( ) Sketch of Incident Area ( ) USB Thumb drive, undated	VINCENT K. MCMAHON Special Agent A Co, 307th MI Bn

E-73. **Signature block.** The signature block follows paragraph 2. The signature block is placed five lines below the last line of text with the first letter centered on the page. It is mandatory that there are at least two lines of text before the signature block. Line one of the signature block is the CI special agent's name in capitalized letters. Line two consists of the words "Special Agent", and line three is the unit of assignment.

VINCENT K. MCMAHON
Special Agent
A Co, 307th MI Bn

CLASSIFICATION

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

1. (X//XX) On 7 December 2008, Brenda Anne RIVERA; SSG; SSN: 123-45-6789; DPOB: 12 March 1976; Pittsburgh, Pennsylvania; Plans Noncommissioned Officer, Room 5, Building 52204, Headquarters (HQ), 1st Signal Brigade (Bde), Fort Huachuca (FH), Arizona; assigned to Headquarters and Headquarters Company (HHC), 1st Signal Bde, FH; residing at Apartment 105, Mountain View Apartment Complex, 800 Carmichael, Sierra Vista, AZ 85635; ETS: 15 June 2008; PCS: 15 June 2008; Security Clearance: TOP SECRET; with daily access to SECRET; Special access: SENSITIVE COMPARTMENTED INFORMATION; SUBJECT 1 of this investigation, provided information concerning HER possible involvement in espionage, the deliberate mishandling of classified information, and HER relationship with Roberto "The Plumber" AMOROS, a Cuban Intelligence Service officer described as follows: SEX: Male; RACE: Hispanic; SKIN COLOR: Light tan; SKIN COMPLEXION: Clear; AGE: 30 - 35; HEIGHT: 5' 11' - 6' 1'; WEIGHT: 160 - 170 pounds; BUILD: Medium; HAIR: Brown, short; EYES: Brown; DRESS: Light blue, short sleeve dress shirt, tan slacks, brown leather belt and dress shoes.

DERIVED FROM: Sec 2-2, Chapter 2, INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 2 DEC 96

CLASSIFICATION

Figure E-2. Example of an IMFR—interview

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

DISTINGUISHING CHARACTERISTICS: Spoke English without an accent; NFI; SUBJECT 2 of this investigation. SUBJECT 1 understood and waived HER rights under Article 31, UCMJ. SUBJECT 1 executed a DA Form 3881 (Rights Warning Procedure/Waiver Certificate). SUBJECT 1 admitted SHE purposely attempted to compromise classified national defense information and release it to SUBJECT 2, who tasked HER to do so. SHE provided the following information concerning the alleged incident:

a. (X//XX) At approximately 1600, 19 May 2008, SUBJECT 1 checked the office, Room 5, Building 52204, HQ, 1st Signal Bde, FH, to make sure SHE was alone. There was no one else in the room. SHE did not want anyone to see HER place the classified flash memory drive in the trashcan. The flash memory drive was approximately 2 inches long, 1 inch wide, and 1/2 inch thick. Printed in black on the flash memory drive were the words Centron Spin Drive 4 GB. Affixed to the flash memory drive was a red SECRET classification label approximately one-third inch wide. There was a black cloth lanyard attached to it with red embroidered stenciling that read 1st Signal Brigade General Defense Plan 06-01 (U). The General Defense Plan (GDP) contained on the flash memory drive was classified SECRET with a NOT RELEASABLE TO FOREIGN NATIONALS handling caveat. The GDP contained information concerning how all units stationed at FH would react to various forms of attack or emergency. The GDP also contained units located outside FH who would quickly deploy to FH. Because the document focused on FH's defense, it identifies strategic and tactical weaknesses concerning FH. SUBJECT 1 knew that compromising the GDP could result in grave damage against FH facilities, operations, and personnel. There were no other files on the flash memory drive.

CLASSIFICATION

Figure E-2. Example of an IMFR—interview (continued)

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

b. (X//XX) SUBJECT 1 removed the flash memory drive from HER computer and placed it in HER trashcan located at the front, right hand corner of HER desk. SUBJECT 1 was very nervous and forgot to place other trash on top of the flash memory drive. SUBJECT 1, although SHE had poor organizational skills, never purposely mishandled classified information before and started to feel physically ill. SUBJECT 1 kept a cluttered desk, as usual, and SHE thought about how easily the flash memory drive could accidentally fall or how someone could knock it into HER trashcan. SHE decided that was how she would explain it if something went wrong and someone found it in the trashcan before SUBJECT 2 retrieved it. SUBJECT 1 shut down HER computer, locked the security container, and initialed the SF 702 (Security Container Checksheet) on top on the container. SUBJECT 1 knew, since it was Friday, someone from the office would conduct the end of day security checks and clean up, to include taking all the office trash out to the dumpster.

c. (X//XX) At approximately 1615, SUBJECT 1 turned HER computer off and left the office. SHE walked out to the parking lot to HER privately owned vehicle (POV), entered it, and drove to HER residence. At approximately 1645, SUBJECT 1 arrived at HER residence. SUBJECT 1 was very concerned because SHE knew SHE forgot to cover the flash memory drive with other trash. SUBJECT 1 was also worried that SUBJECT 2 would be very angry when HE found out SHE did not cover up the flash memory drive. SUBJECT 1 wanted to call SUBJECT 2, but HE told HER not to call HIM because HE would contact HER after a few days went by. SUBJECT 1 went about HER normal daily schedule and waited for SUBJECT 2 to contact HER.

d. (X//XX) SUBJECT 1 first met SUBJECT 2 in November 1998, exact date not recalled, at an off-post restaurant in Vilseck, Germany. From November 1998 to February 1999, exact dates not recalled, SUBJECT 1 and SUBJECT 2 met socially at various locations, at least once a week, in and around Vilseck. In mid-February 1999, exact date not recalled, SUBJECT 1 and SUBJECT 2 were romantically involved.

CLASSIFICATION

Figure E-2. Example of an IMFR—interview (continued)

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

SUBJECT 2 appeared very interested in SUBJECT 1, asking HER many questions about HER life and job. SUBJECT 2 bought gifts for SUBJECT 1 including jewelry, stuffed animals, and romantic greeting cards. SUBJECT 1 was very happy with the growing relationship and believed SHE was very fortunate because SUBJECT 2 seemed very interested in HER feelings and even HER career. SUBJECT 2 told SUBJECT 1 HE worked local jobs as a woodworker and applying finishes to furniture. SUBJECT 2 rented a small apartment in Vilseck but preferred to meet SUBJECT 1 at other locations, usually a gasthaus. A gasthaus was a small bar/restaurant which rents out a few rooms.

e. (X//XX) SUBJECT 2 did not ask SUBJECT 1 for any classified or unclassified national defense information while in Vilseck. SUBJECT 2 did ask questions about SUBJECT 1's job and even HER security clearance level. SUBJECT 1 told HIM SHE held a TOP SECRET clearance, but usually only handled SECRET information. SUBJECT 1 told SUBJECT 2 SHE was excited because HER next duty assignment in Fort Lewis, Washington, would allow HER to work on more "high speed" projects. SUBJECT 1 often started conversations about what SHE did at work because SUBJECT 2 always became very attentive when SHE talked about work. While stationed in Vilseck, SUBJECT 1 never spoke to SUBJECT 2 about classified information or sensitive operational information. SUBJECT 1 did discuss information contained in UNCLASSIFIED Army Regulations an Field Manuals. SUBJECT 1 could [provide no further pertinent information concerning the information she discussed with SUBJECT 2.

f. (X//XX) In March 2000, exact date not recalled, SUBJECT 1 traveled to HER new assignment in Fort Lewis, while SUBJECT 2 moved nearby so THEY could be together. SUBJECT 1 was assigned to 3rd Bde, 2d Infantry Division, Fort Lewis. SUBJECT 1 worked as an instructor at the System Administrator & Network Manager's Security Course.

CLASSIFICATION

Figure E-2. Example of an IMFR—interview (continued)

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

SUBJECT 2 told SUBJECT 1 HE obtained employment with a local plumbing company. SUBJECT 1 had almost daily social contact with SUBJECT 2 and no professional contact. From June 2000 to July 2003, exact dates not recalled, SUBJECT 1 and SUBJECT 2 continued THEIR romantic relationship. SUBJECT 2 remained very interested in SUBJECT 1's work. SUBJECT 2 often asked to see the training material SUBJECT 1 used to teach system administration and network security. SUBJECT 1 often brought UNCLASSIFIED instructional material back to HER barracks room to prepare to instruct classes. SUBJECT 2 told SUBJECT 1 HE could help HER study the material by asking HER questions and using the instructional material to make sure SHE knew the correct answer. The materials which SUBJECT 2 helped SUBJECT 1 review were: System Administration Level 1(U), System Administration Level 2(U), Network Security Level 1(U), Network Security Manager Level 1(U), all UNCLASSIFIED. These instructional manuals covered basic file manipulation, UNIX operating system, UNIX basic commands, UNIX and Windows networking, and UNIX and Windows security.

g. (X//XX) In August 2002, exact date not recalled, SUBJECT 1 asked SUBJECT 2 to move in with HER because SHE loved HIM and wanted to know what it would be like to live with HIM. SUBJECT 2 said HE was not ready for that step, but that HE did love HER and thought THEIR relationship was great as it was. SUBJECT 1 and SUBJECT 2 continued THEIR romantic relationship.

h. (X//XX) In July 2003, exact date not recalled, SUBJECT 1 was assigned to 78th Signal Bn, Camp Zama, Japan. SUBJECT 2 traveled to Tokyo (coordinates not available), Japan and found work as a handyman. SUBJECT 1 and 2 had weekly social contact and no professional contact. SUBJECT 1 and SUBJECT 2 continued THEIR romantic relationship.

CLASSIFICATION

Figure E-2. Example of an IMF—interview (continued)

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

SUBJECT 2 became increasingly distant over time toward SUBJECT 1. SUBJECT 2 met less with SUBJECT 1 from July 2003 to April 2004. SUBJECT 2 often narrowed discussion topics to SUBJECT 1's work. If SUBJECT 1 talked about work, SUBJECT 2 would show increased affection. This resulted in SUBJECT 1 initiating more conversations surrounding HER work. SUBJECT 2 asked SUBJECT 1 to bring HIM Field Manuals and other publications dealing with communications and automated information systems SHE used at work. The material, SUBJECT 1 brought SUBJECT 2 was UNCLASSIFIED. SUBJECT 1 began to feel uncomfortable about how interested SUBJECT 2 was in HER job and asked HIM why HE wanted to see so much material. SUBJECT 2 told SUBJECT 1 HE was proud of the work SHE did and was so interested because HE cared about HER. SUBJECT 1 could provide no further pertinent information concerning the material SHE provided to SUBJECT 2.

i. (X//XX) On 7 February 2005, SUBJECT 2 called SUBJECT 1 and told HER to meet HIM at a motel. SUBJECT 1 went to the motel and met with SUBJECT 2. SUBJECT 2 said HE did not want anyone to see HIM in public with HER and would call HER to arrange meetings at motels. SUBJECT 2 told SUBJECT 1 to get rid of all pictures and anything else that showed a connection between THEM. SUBJECT 1 started to cry and asked HIM why HE wanted HER to do that. SUBJECT 2 told HER HE worked for the Cuban Intelligence Service and HE wanted HER to collect classified information for HIM. SUBJECT 1 told SUBJECT 2 SHE thought HE loved HER. SUBJECT 2 told SUBJECT 1 HE did love HER and SHE needed to listen to HIM and do what HE wanted. SUBJECT 1 told SUBJECT 2 SHE could not give HIM classified information. SUBJECT 2 told SUBJECT 1 SHE had already given HIM a great amount of information and if SHE did not do what HE wanted, HE would turn HER into the authorities.

CLASSIFICATION

Figure E-2. Example of an IMFR—interview (continued)

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

SUBJECT 2 said SHE had an affair with a foreign intelligence agent and the authorities would never believe SHE did not know who HE was. SUBJECT 1 agreed to do what SUBJECT 2 wanted. SUBJECT 1 felt betrayed by SUBJECT 2 but still loved HIM and was afraid to disobey HIM. SUBJECT 2 continued to meet with SUBJECT 1 occasionally. SUBJECT 1 informed SUBJECT 2 HER next duty station was FH. SUBJECT 2 appeared happy and told HER HE would also move nearby sometime after SHE arrived there. SUBJECT 1 could provide no further pertinent information concerning HER meetings with SUBJECT 2.

j. (X//XX) In June 2005, exact date not recalled, SUBJECT 1 was assigned to HHC, 1st Signal Bde. In early July 2005, exact date not recalled, SUBJECT 2 called SUBJECT 1 and told HER to meet HIM at the Days Inn Conference Center, 222 South Freeway Road, Tucson, AZ 85745, on 8 July 2008. SUBJECT 2 told SUBJECT 1 HE would call HER the day before and give HER HIS room number.

k. (X//XX) On 8 April 2008, SUBJECT 1 drove HER POV to Tucson and met SUBJECT 2 in Room 34 at Days Inn. SUBJECT 1 was very happy to see SUBJECT 2, but SUBJECT 2 was cold to HER and questioned HER extensively about HER new workplace and what information SHE had access to. SUBJECT 2 told HER to look through all the classified material SHE had access to. SHE was to do this over time and only when no one else was around. SHE was to remember titles of documents and know what type of information they contained. SHE was not to call HIM unless it was an emergency, and SHE could not tell anyone about HIM. HE called HER occasionally to set up meetings. SUBJECT 2 told HER to do a good job at work and to not do anything that would negatively affect HER access to classified information. SUBJECT 2 asked SUBJECT 1 if SHE understood all the instructions and SHE said yes. SUBJECT 1 could provide no further pertinent information.

CLASSIFICATION

Figure E-2. Example of an IMFR—interview (continued)

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

l. (X//XX) Between July 2005 and January 2008, SUBJECT 1 followed SUBJECT 2's instructions and became familiar with most of the classified information stored in HER office. Once every few weeks, exact dates not recalled, SUBJECT 2 called SUBJECT 1 and arranged meetings at random motels in Tucson during the weekends. SUBJECT 1 briefed SUBJECT 2 on the classified material SHE had access to. This access was limited as HER position did not warrant a need to know. In January 2008, exact date not recalled, SUBJECT 1 became the Plans Noncommissioned Officer. This position required daily access to classified material. SUBJECT 1 could provide no further pertinent information.

m. (X//XX) In early April 2008, SUBJECT 1 met SUBJECT 2 at a motel in Tucson. THEY discussed HER new position and access. SUBJECT 2 showed interest in the 1st Signal Brigade General Defense Plan 06-01 (U). SUBJECT 1 told HIM they kept the document on a classified flash memory drive. THEY discussed ways to remove the flash memory drive from SUBJECT 1's office. SUBJECT 1 said SHE would feel very uncomfortable leaving the office with the flash memory drive or any other classified material in HER possession. SUBJECT 2 asked HER when they took the trash out of the office. SHE told him that every Friday, junior enlisted Soldiers removed all the trash in HER office and took it to the dumpster out in the parking lot. SUBJECT 2 smiled and said HE knew exactly how THEY would remove the classified information. HE told HER HE had access to a trash truck and should be able to get it onto post. SUBJECT 2 told HER to place the flash memory drive into a trashcan in HER office and cover it up with trash so no one would know it was there. SUBJECT 2 would drive the trash truck onto post that night and remove all the trash in the dumpster. That way SUBJECT 1 did not have to take the chance of removing the material HERSELF. SUBJECT 2 told HER HE would contact HER when HE wanted HER to do it. SUBJECT 1 could provide no further pertinent information.

CLASSIFICATION

Figure E-2. Example of an IMFR—interview (continued)

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

n. (X//XX) On 18 May 2008, SUBJECT 2 called SUBJECT 1 and asked if the Friday trash procedures had changed; SUBJECT 1 said no. SUBJECT 2 told HER to make it happen on 19 May 2008 and SUBJECT 1 said SHE would. On 22 May 2008, exact time not recalled, SUBJECT 1 found the flash memory drive in the security container. As time passed and no one said anything to HER, SHE believed no one knew it was HER who put it in the trash can. It concerned HER that SUBJECT 2 had not contacted HER since 18 May 2008. SHE was worried about HIM and wondered if HE was angry with HER because HE did not receive the flash memory drive.

o. (X//XX) On 20 August 2008, SUBJECT 2 called SUBJECT 1 and arranged a meeting for 2 September 2008, at the Lucky Star Motel, 23 Lucy Way, Santa Fe, New Mexico. SUBJECT 2 told SUBJECT 1 to request leave for a trip to Las Vegas, Nevada and go there for a few days then drive to meet HIM on 2 September 2008. On 21 August 2008, SUBJECT 1 requested leave from 31 August 2008 to 6 September 2008, to go to Las Vegas. On 31 August 2008, SUBJECT 1 drove to Las Vegas and spent two nights at the Royal Dove Hotel and Casino, 147 Paramount Ave, Las Vegas. During this time SUBJECT 1 spent $200 (US) gambling, watched the hotel shows, and spent the rest of HER time in HER room wondering how the meeting would go with SUBJECT 2. SUBJECT 1 was still worried that somehow, someone would find everything out.

p. (X//XX) In the early morning, 2 September 2008, exact time not recalled, SUBJECT 1 drove to Santa Fe and met SUBJECT 2. SUBJECT 1 began to cry and told SUBJECT 2 SHE was sorry it did not work. SUBJECT 2 hugged HER and told HER it was OK and THEY would find another way to do it. To SUBJECT 1's surprise, SUBJECT 2 was very affectionate and steered the conversation toward THEIR relationship and talked about showing HER around town. From 2 September 2008 to 4 September 2008, SUBJECT 1 and SUBJECT 2 spent the entire time together and continued THEIR romantic relationship.

CLASSIFICATION

Figure E-2. Example of an IMFR—interview (continued)

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

SUBJECT 2 said nothing about what HE wanted SUBJECT 1 to do next at work. SUBJECT 2 said not to worry and everything was fine. SUBJECT 2 said it was not SUBJECT 1's fault. SUBJECT 2 told SUBJECT 1 HE would contact HER in a few weeks; HE did not give a specific date. SUBJECT 1 could provide no further pertinent information.

q. (X//XX) On 15 October 2008, SUBJECT 2 called SUBJECT 1 and told HER HE needed to go on a trip, but would be back in about a month. SUBJECT 2 told SUBJECT 1 HE loved HER and HE would call HER as soon as HE returned. SUBJECT 1 asked where SUBJECT 2 would be, but HE did not reply. SUBJECT 2 had not contacted SUBJECT 1 since the 15 October 2008 phone call.

r. (X//XX) SUBJECT 1 complained at work about not having enough money because SHE believed SHE should make more money with the computer and networking skills SHE had. SUBJECT 1 could provide no further pertinent information.

s. (X//XX) SUBJECT 1 had poor organizational skills at work. SHE worked on a large number of projects at one time and it was hard to keep up on them all. SUBJECT 1 could provide no further pertinent information.

t. (X//XX) SUBJECT 2 told SUBJECT 1 HE was a Cuban Intelligence Service agent and HE focused on collecting information from US Military personnel and facilities. SUBJECT 1 could provide no further pertinent information.

u. (X//XX) SUBJECT 1 could provide no pertinent information concerning SUBJECT 2's financial matters, work habits, personal conduct, outside activities, foreign considerations, or emotional/mental/personality disorders.

CLASSIFICATION

Figure E-2. Example of an IMFR—interview (continued)

CLASSIFICATION

ATZS-TPQ-A 8 December 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Espionage
19 May 2008 (X//XX)
ASCCN: 06-902d-357 (U)

v. (X//XX) Source executed a DA Form 2823, Sworn Statement, read and signed a Secrecy Affirmation Statement and was advised of the four salient points of the Privacy Act of 1974.

2. (X//XX) AGENT'S COMMENTS: Agent names and any other personal identifying information are exempt from release under FOIA exemptions 6 and 7 (civilians: 5 USC §§ 552(b)(6) and (b)(7)(c)) and may not be disclosed in response to FOIA requests for IIRs or other intelligence investigative documents.

EXHIBIT
( ) DA Form 2823
( ) DA Form 3881

JUSTIN J. BLACK
Special Agent
A Co, 307th MI Bn

CLASSIFICATION

Figure E-2. Example of an IMFR—interview (continued)

CLASSIFICATION

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

ATZS-TPQ-A 22 May 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM OFFICIAL MILITARY PERSONNEL RECORDS

1. (X//XX) On 22 May 2008, a review of the Personnel File available at 1st Signal Brigade, Fort Huachuca, Arizona 86513, provided information regarding Brenda Anne RIVERA, SSG, 123-45-6789, DPOB: 12 March 1976, Pittsburgh, Pennsylvania; SUBJECT 1 of this investigation. The purpose of this review was to determine previous and current assignments, security information, special skills, and previous access to special technology or projects. The checks revealed the following information:

NAME:	RIVERA, Brenda Anne
RANK:	SSG
SSN:	123-45-6789
DPOB:	12 March 1976, Pittsburgh, PA

DERIVED FROM: Sec 2-2, Chapter 2, INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 2 DEC 96

CLASSIFICATION

Figure E-3. Example of an IMFR—personnel files checks

CLASSIFICATION

ATZS-TPQ-A 22 May 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

DUTY POSITION:	Plans Noncommissioned Officer
HOME ADDRESS:	Apartment 105, Mountain View Apartment Complex, 800 Carmichael Sierra Vista, Arizona 85635
HOME OF RECORD:	Pittsburgh, PA
MARITAL STATUS:	Single
PEBD/BASD:	1 April 1998/1 June 1998
PMOS/SMOS:	25D30
ASSIGNMENTS:	June 2005–Present; 1st Signal Bde, Fort Huachuca, AZ July 2003–June 2005; 78th Signal BN, Camp Zama, Japan June 2000–July 2003; 3d Bde, 2d Inf Div, Fort Lewis, Washington June 1998–June 2000; HHC 94th Eng Bn, 130th Eng Bde Vilseck, Germany

CLASSIFICATION

Figure E-3. Example of an IMFR—personnel files checks (continued)

CLASSIFICATION

ATZS-TPQ-A 22 May 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

MILITARY EDUCATION:	May 2003; BNCOC, Fort Carson, Colorado June 2000; Primary Leadership Course, Fort Campbell, Kentucky January 1998–June 1998; AIT, Fort Gordon, Georgia
PCS:	June 2008
SECURITY CLEARANCE:	JPAS [Joint Personnel Adjudication System] revealed a TOP SECRET clearance issued by CCF on 14 June 1998. Clearance based on an SSBI completed by DIS on 14 May 1998
DEROGATORY INFORMATION:	None
CIVILIAN EDUCATION:	September 1990 to June 1994; North West High School, Pittsburgh, PA
CIVILIAN EMPLOYMENT:	None listed
ETS:	26 April 2008

CLASSIFICATION

Figure E-3. Example of an IMFR—personnel files checks (continued)

CLASSIFICATION

ATZS-TPQ-A 22 May 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

2. (X//XX) AGENT'S NOTES: Agent names and any other personal identifying information are exempt from release under FOIA exemptions 6 and 7 (5 USC §§ 552(b)(6) and (b)(7)((c)) and may not be disclosed in response to FOIA requests for IIRs or other intelligence investigative documents. Abbreviations in this report are as they appear in the SUBJECT's Personnel File. Harry D. Burke, SPC, record custodian for 1st Signal Bde provided the file for review.

EXHIBIT A

JUSTIN J. BLACK
Special Agent
A Co, 307th MI Bn

CLASSIFICATION

Figure E-3. Example of an IMFR—personnel files checks (continued)

CLASSIFICATION

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

ATZS-TPQ-A 15 June 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
9 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM OFFICIAL GOVERNMENT RECORDS

1. (X//XX) On 21 May 2008, a review of the Pass and Identification Office files available at Main Gate, Fort Huachuca, Arizona 86513, provided information regarding Roberto MNU AMOROS; SUBJECT 2 of this investigation. The purpose of this review was to determine SUBJECT 2's identity and reason for being on Fort Huachuca. The checks revealed the following information:

a. (X//XX) SUBJECT 2 entered Fort Huachuca on 17 April 2008, 22 May 2008, 19 June 2008. SUBJECT 2 drove the same Cochise Disposal Systems truck every time HE entered Fort Huachuca. On 17 April 2008, SUBJECT 2 told the civilian security guard at the main gate HE applied for an Arizona commercial license plate at the Motor Vehicles Division, Sierra Vista, AZ. SUBJECT 2 had no license plate on the truck.

b. (X//XX) SUBJECT 2 also told the civilian security guard HE checked into the Windemere Hotel and Conference Center, Sierra Vista, each time he traveled to Fort Huachuca.

DERIVED FROM: Sec 2-2, Chapter 2, INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 2 DEC 96

CLASSIFICATION

Figure E-4. Example of an IMFR—records checks

CLASSIFICATION

ATZS-TPQ-A 15 June 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

c. (X//XX) SUBJECT 2 had a New Mexico Driver's license listing HIS permanent address as 4347 Cerrillos Streets, Santa Fe, NM 87507.

2. (X//XX) AGENT'S NOTES: Agent names and any other personal identifying information are exempt from release under FOIA exemptions 6 and 7 (5 USC §§ 552(b)(6) and (b)(7)((c)) and may not be disclosed in response to FOIA requests for IIRs or other intelligence investigative documents. Ned F. Landors, CIV, DOD Security Personnel for Provost Marshal's Office provided the file for review.

EXHIBIT
as

JUSTIN J. BLACK
Special Agent
A Co, 307th MI Bn

CLASSIFICATION

Figure E-4. Example of an IMFR—records checks (continued)

CLASSIFICATION

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

ATZS-TPQ-A 10 June 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM OFFICIAL GOVERNMENT RECORDS

1. (X//XX) On 10 June 2008, a review of files provide by Theater CI Coordinating Authority (ATCICA), originating from Detachment 14, Foreign CI Activity, Intelligence and Security Command, Fort Meade, Maryland, provided information regarding Roberto MNU AMOROS; SUBJECT 2 of this investigation. The purpose of this review was to determine SUBJECT 2's identity and possible connection with foreign entities. The checks revealed the following information:

a. (X//XX) SUBJECT 2 was an Intelligence Officer in the Cuban Intelligence Service (CIS) known as "The Plummer". CIS used "honey pot" operations against unsuspecting female subjects. This typically included the CIS officer building a romantic relationship over a long period of time before revealing their true motive. CIS also preferred to use low-budget, low-technology intelligence operations, such as pay telephones, secure communications plans, dead drops, or face-to-face.

DERIVED FROM: Sec 2-2, Chapter 2, INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 2 DEC 96

CLASSIFICATION

Figure E-5. Example of an IMFR—intelligence files checks

CLASSIFICATION

ATZS-TPQ-A 10 June 2008

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

b. (X//XX) SUBJECT 2's prior actions include building relationships with female Soldiers and civilians who worked on Fort Campbell, Kentucky in 1996. SUBJECT 2 began romantic relationships with, and elicited unclassified military operational and personnel information from these individuals. US Army Intelligence discovered these actions in late 1996 but SUBJECT 2 left the area shortly after, location unknown.

c. (X//XX) SUBJECT 2's last known residence was Lot 12, 202 N. Wellspring Drive, New Horizons Trailer Park, Clarksville, Tennessee. Record Checks indicated SUBJECT 2 rented a trailer from February 1996 to October 1996 and paid in cash.

2. (X//XX) AGENT'S NOTES: Agent names and any other personal identifying information are exempt from release under FOIA exemptions 6 and 7 (5 USC §§552(b)(6) and (b)(7)((c)) and may not be disclosed in response to FOIA requests for IIRs or other intelligence investigative documents. John J. Walker, CW4, Operations Officer, 902nd ATCICA Office CONUS, provided the file for review.

EXHIBIT
as

JUSTIN J. BLACK
Special Agent
A Co, 307th MI Bn

CLASSIFICATION

Figure E-5. Example of an IMFR—intelligence files checks (continued)

CLASSIFICATION

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

ATZS-TPQ-A 10 June 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM OFFICIAL PUBLIC RECORDS

1. (X//XX) On 10 June 2008, a check of the following agencies' records revealed no information identifiable with Brenda A. RIVERA, SSG, 123-45-6789; DPOB: 12 March 1976, Pittsburgh, Pennsylvania; SUBJECT 1 of this investigation. The purpose of this check was to determine if SUBJECT was ever involved in any criminal activity which would explain HER suspected involvement with a known Foreign Intelligence Officer.

a. (U) Sierra Vista Police Department, Sierra Vista, Arizona

b. (U) Tucson Police Department, Tucson, AZ

c. (U) Cochise County Sheriff's Office, Sierra Vista

DERIVED FROM: Sec 2-2, Chapter 2, INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 2 DEC 96

CLASSIFICATION

Figure E-6. Example of an IMFR—law enforcement records checks

CLASSIFICATION

ATZS-TPQ-A 10 June 2008

INVESTIGATIVE MEMORANDUM FOR RECORD

SUBJECT: Fort Huachuca, Arizona
Security Matter (Compromise)
19 May 2008 (X//XX)
LCCN: 06-Team 9-001 (U)

2. (X//XX) AGENT'S NOTES: Agent names and any other personal identifying information are exempt from release under FOIA exemptions 6 and 7 (5 USC §§ 552(b)(6) and (b)(7)((c)) and may not be disclosed in response to FOIA requests for IIRs or other intelligence investigative documents.

EXHIBIT
as

JUSTIN J. BLACK
Special Agent
A Co, 307th MI BN

CLASSIFICATION

Figure E-6. Example of an IMFR—law enforcement records checks (continued)

REPORT OF INVESTIGATION

E-74. The report of investigation (ROI) serves as an executive summary of investigative results reported in IMFRs and Exhibits. The ACICA processes and forwards investigative and operational records included in the ROI to the Investigative Records Repository (IRR), Fort Meade, MD. ROIs are required for any investigation that goes beyond the interview(s) of the original source(s) of information and local and military agency checks (Standing Investigative Authority).

E-75. The ROI highlights investigative efforts to either confirm or discount espionage indicators or allegations. The report should be concise, ensuring pertinent results are emphasized. The agent preparing the ROI cites investigative findings to explain, refute, or support allegations or incidents in which espionage activity is suspected.

SUSPENSE DATES

E-76. Regulatory Requirements: AR 381-12 mandates that the ROI will be submitted to ACICA within 45 days of the termination of the investigation. ACICA may grant ATCICA an extension, upon request.

E-77. ATCICA Suspense Dates: When the ATCICA terminates an investigation, it will task the appropriate element to prepare and submit an ROI. **In most cases, the suspense for the ROI to reach the ATCICA is 30 days after the termination date**. If an investigation involved minimal investigative activity, ATCICA may issue a shorter suspense for the ROI. If an investigation has been lengthy and contained a significant amount of investigative activity, ATCICA may extend the suspense for the ROI.

E-78. Transmission of ROI: The ROI and all original signature documentation must be sent through command channels and received by ATCICA before the assigned suspense. Regardless of the electronic medium used, the ROI and all administrative documents pertaining to the ROI (for example, exhibit cover sheets and multiple source classification listings) must be included.

E-79. ROI Review and Approval Process: The ATCICA will review the ROI and forward the ROI to the ATCICA. The ATCICA reviews the ROI and coordinates with the ATCICA to resolve any discrepancies or problems with the document. The ATCICA will publish a message closing the investigation and retire the ROI to the intelligence records repository.

E-80. Interim ROIs: Interim ROIs are required when a case is being transferred from one office to another or from one ATCICA's AOR to another ATCICA's AOR.

INITIATING THE REPORT OF INVESTIGATION

E-81. Once an investigation is opened and a lead investigative element is assigned, the lead investigating element will begin drafting the ROI. The administrative portions of the ROI will be prepared once the investigating unit receives the ATCICA opening message.

E-82. Each time an investigative action takes place and an IMFR completed, the lead agent will prepare an ROI entry summarizing the action and its implications for the case. This ROI-in-progress can serve as a running case status report and drastically reduce the amount of time required to complete the ROI upon case termination.

E-83. By writing the ROI as the investigation progresses, instead of writing it at the conclusion of the case, the lead agent will save time and effort since more than three quarters of the work on the ROI will be completed by the time the investigation is terminated. When the investigation is terminated, the lead agent will only review and consolidate investigative actions as required, fine tune the report, attach original signature documents, and forward the ROI through command channels to the ATCICA.

FORMAT

E-84. The ROI is prepared using a standardized format on letterhead stationary from the lead investigative unit. The required print style is letter quality, Courier New font, 12 pitch font size. Use normal margins on continuation pages with the page sequential numbers centered at the bottom of each continuation page. If additional pages are required, use plain bond paper.

E-85. **Administrative heading.** The administrative heading consists of the lead investigative element's office symbol, the date prepared (the completed ROI) and the type of report. At the top of each continuation page, place the office symbol on the top line, left margin, and the date prepared at the right margin. On the second line, place the ACICA CCN.

CLASSIFICATION

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

IAMG-A-A 25 November 2004

REPORT OF INVESTIGATION

CLASSIFICATION

IAMG-A-A 25 November 2004

ACICA CCN: 05-5555-902 (U)

E-86. **Paragraph 1, administrative data.** Paragraph 1 of the ROI consists of the administrative data, which can usually be extracted from the CI incident report and the ACICA response. Paragraph 1 of the ROI consists of the investigation title and the ACICA CCN (as reflected on the ACICA opening message), command investigating the incident, control office, date opened, date closed (left blank), the reason for investigation and the case status (terminated, transferred or suspended). The second example below is for identifying the reason the investigation was initiated.

1. (X) ADMINISTRATIVE DATA:

TITLE: SMITH, John D.
ACICA CCN: 05-5555-902
CPT, 123-45-6789
15 June 1973, Omaha, NE

INVESTIGATING UNIT: 902d MI Group
CONTROL OFFICE: ATCICA
DATE OPENED: 4 October 2004
DATE CLOSED:

REASON FOR INVESTIGATION: To determine if CPT John D. SMITH engaged in espionage on behalf of an FISS and ITO or a foreign government as indicated by HIS unreported continuing contact with foreign military officers and HIS unauthorized removal of classified documents from a secured area.

CASE STATUS: Terminated

To determine if Ann B. AAAAA engaged in espionage on behalf of a foreign intelligence service or a foreign government, as indicated by HER alleged impersonation of a MI special agent.

To determine if Michael C. BBBBB engaged in espionage on behalf of a foreign intelligence service or a foreign government, as indicated by HIS failure to complete a CI Scope Polygraph Examination.

To determine if David D. CCCCC had unauthorized contact with a representative of a foreign intelligence service or a foreign government or compromised classified defense information while Absent Without Leave.

To determine if the circumstances surrounding the suicide of Fanny O. DDDDD indicated HER involvement in espionage activity on behalf of a foreign intelligence service or a foreign government.

To determine if Bartholomew O.J. EEEEE III committed a Communications Security (COMSEC) violation under the direction of a foreign intelligence service or a foreign government.

To determine if Jane K. FFFFF had an unauthorized contact with a representative of a foreign intelligence service or a foreign government for the purposes of espionage activity.

E-87. **Paragraph 2, synopsis.** Paragraph 2 contains a summary of the investigative results reported in the IMFR. It is a concise summary of the elements of an investigation. The ROI should address the basic interrogatives, which were answered during the progress of the investigation concerning the SUBJECT and the incident. In the case of CI scope polygraph examination (CSPE) investigations, this subparagraph will contain a synopsis of the information provided by the polygraph packet and the ATCICA opening memorandum.

E-88. **Privacy Act Caveats.** The first entry of Paragraph 2 preceding subparagraph a will be all appropriate Privacy Act caveats, which may restrict the release of the investigative information. List all appropriate caveats between the paragraph heading and the narrative. Capitalize and center the listed caveats. The ROI will list a caveat when the information was obtained from—

- Financial Institutions (AR 190-6).
- Electronic Surveillance (AR 381-10, chapter 5).
- Source Requesting Confidentiality.
- A governmental agency which requires consent for the release of its information.

2. (U) SYNOPSIS:

SOURCE WAS GIVEN AN EXPRESSED PROMISE OF CONFIDENTIALITY
AS A CONDITION OF PROVIDING INFORMATION IN THIS REPORT

INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM A
FEDERAL AGENCY, WHO RESERVES THE RIGHT TO RESTRICT RELEASE
INFORMATION CONTAINED IN THIS REPORT IS FINANCIAL RECORD INFORMATION, WHICH WAS OBTAINED PURSUANT TO THE RIGHT OF FINANCIAL PRIVACY 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

E-89. **First subparagraph.** The first subparagraph of paragraph 2 contains the essence of the information reported in the CI incident report. It contains the date the information was reported, identification of the source, full identification of the SUBJECT, unit of assignment, and an outline of the allegations upon which the investigation was predicated. Identifying data for all subjects will include Name, rank, SSN, DPOB, duty position, name of unit or organization and location of unit. Other persons involved in the investigation (for example, source, witnesses, co-workers) will be identified only by their full name and relationship to the investigation (for example, source, SUBJECT's neighbor, co-worker). Any reference to SUBJECT or SUBJECT's last name will be typed in capital letters. This paragraph must also contain a statement as to when ATCICA opened the case.

a. (X) This investigation was predicated on the 2 October 2004, report that under a promise of confidentiality David L. Roth, SPC, reported that John David SMITH, CPT, 123-45-6789, DPOB: 15 June 1973, Omaha, NE; 35E, Security Officer, Headquarters and Headquarters Company (HHC), 3rd Battalion, 28th Infantry Regiment, Fort Riley, KS, hereinafter referred to as SUBJECT, removed classified information from the safe located in the S-2 of 3/28 INF BN headquarters building, placed the information in HIS coat pocket and departed the building. SUBJECT often told source about HIS new girlfriend and commented that HE would like to learn Russian so that HE would be able to communicate with her better. On 4 October 2004, ATCICA opened this investigation. (1,2, Exhibit I)

E-90. **IMFR/Exhibit numbering.** This and subsequent subparagraphs referring to investigative results reported in the IMFRS and supported by the exhibits will reference the appropriate documentation from which the information was extracted for synopsis at the end of the subparagraph. An Arabic numeral in parentheses references IMFRs at the end of each summary paragraph, and exhibits are referenced by Roman numerals. Do not place the numerals on the reports or exhibits until the ROI is complete. Then, *IN PENCIL*, write the numerals on the bottom right of the first page of the IMFRs and on the bottom center of the exhibit cover sheet. This first subparagraph must summarize the CI incident report and ATCICA opening message. In the case of a CSPE investigation, the ATCICA memorandum will act as the reference.

E-91. Subsequent subparagraphs will synopsize the investigative actions conducted to support, refute, or mitigate the information reported in the CI incident report. Similar investigative actions with similar results may be summarized in the same subparagraph. The subparagraphs of the ROI should follow the logical flow of the case's development. This does not mean to always set a chronological pattern of events. List IMFRS and Exhibits to flow sequentially.

b. (X) From 5 October 2004 to 15 October 2004, interviews of SUBJECT's co-workers and supervisors provide background and personal information concerning SUBJECT, but nothing pertinent to this investigation. (2-5)

c. (X) On 15 October 2004, Robert R. Truit, SUBJECT's neighbor, provided that SUBJECT frequently traveled to Canada on fishing trips. SUBJECT was an avid fisherman. (6, Exhibit II)

d. (X) On 17 October 2004, Jerry P. Jones, SUBJECT's co-worker, provided that SUBJECT used illegal drugs on a weekly basis. Jones witnessed SUBJECT take office manuals to HIS automobile. (7, Exhibit III)

e. (X) From 5 October 2004 to 20 October 2004, civilian and military law enforcement, credit bureau, finance, personnel, and security records provided assignment data, allotment and financial information, but no derogatory information concerning SUBJECT. (8-11)

E-92. **Significant results.** Interviews resulting in significant information will be identified in a separate subparagraph for each interview. Interviews not resulting in significant information will be included in one subparagraph for all similar interviews. This ensures significant interviews stand out to the reader. When an interview includes a Rights Warning, include a statement in the ROI that individuals read and waived or invoked their legal rights.

E-93. **Paragraph 3, case status.** Paragraph 3 indicates the case status and complements information provided in the first paragraph of the ROI. The closing paragraph briefly addresses the investigative results as they pertain to the allegations listed in the opening paragraph. This paragraph will also list actions taken to neutralize any threat, such as revocation of security clearance or prosecution. In the case of interim ROIs, explain the reason for the interim ROI and the basis for continuing the investigation. This paragraph should synopsize any supporting, mitigating, or exculpatory information obtained during the course of the investigation. For example, "The loss of COMSEC material was due to inadvertent destruction" or "The security container had an inoperable locking mechanism which could not be attributed to foul play initiated by a foreign intelligence and security systems (FISS) and international terrorist organizations (ITO)." Computer network incident investigations may need more of an explanation concerning the investigative findings. Recommendations, reviewer's opinions, or conclusions deemed appropriate will be noted in the letter of transmittal accompanying the ROI. **NO such comments will be included within the ROI.**

3. (X) CASE TERMINATED: This investigation did not disclose any indication of espionage activity. John Q. PUBLIC is a certified collector of law enforcement badges and has not falsely identified HIMSELF for any illegal purposes or personal gain.

3. (X) CASE TERMINATED: This investigation did not disclose any indication of espionage activity. John Q. PUBLIC considered the polygraph examination program to be an infringement on HIS right to personal privacy. PUBLIC resigned from HIS position with the Army and no longer has any access to U.S. defense information.

3. (X) CASE TERMINATED: This investigation did not reveal any indication of a foreign intelligence service involvement or evidence of a security compromise committed by John Q. PUBLIC during HIS AWOL period. PUBLIC believed HIS commander was preparing to give HIM an Article 15 for being late to work on several occasions.

3. (X) CASE TERMINATED: This investigation did not disclose any indication of espionage activity. John Q. PUBLIC's suicide was incidental to HIS being jilted by HIS lover.

3. (X) CASE TERMINATED: This investigation did not disclose any indication of espionage activity. John Q. PUBLIC was unaware of others who had access to HIS safe. ATCICA referred this matter to SUBJECT's command for their action.

3. (X) CASE TERMINATED: This investigation determined that John Q. PUBLIC is a U.S. citizen not affiliated with the Department of Defense. ATCICA referred this matter to the Federal Bureau of Investigation for their action.

3. (X) CASE TERMINATED: This investigation did not determine that John Q. PUBLIC engaged in espionage activity on behalf of a FISS and ITO. Under the special authority of the Security Office, PUBLIC is authorized to transport defense information from HIS office to other U.S. Government buildings located on the other side of town.

E-94. **Paragraph 4, preparer.** Paragraph 4 identifies the preparer of the ROI.

4. (U) ROI prepared by: Special Agent Jane A. Quigley, A Company, XXXth Military Intelligence Battalion, 902d MI Group, City, State, Zip Code.

E-95. **Enclosure list.** The enclosure list is placed at the left margin on the same line as the signature block. List the total number of IMFRs and exhibits.

Note. The following documents are NOT included with the ROI: Privacy Act Statements, Secrecy Affirmations, Non-Disclosure Statements, tasking messages, case control sheets, IPs, internal or administrative documents such as telephone memoranda, and planning documents. DO NOT place them as exhibits to IMFRs.

E-96. **Signature block.** The last entry on the ROI will be the signature block of the approving authority. All ROIs will be reviewed by the ATCICA for investigative sufficiency and adherence to ROI guidelines. The lead agent's company commander will sign the ROI.

Encl
16 IMFRs
7 Exhibits

JOHN B. JONES
CPT, MI
Commanding

E-97. **Unlisted attachments.** The requirement for separate unlisted attachments, and the accompanying cover memorandum, no longer exists. Actions which were not strictly investigative in nature but which influenced the course of the investigation were previously documented as unlisted attachments; these actions will now be addressed in the actual ROI. Supporting documentation, which would have previously been handled as unlisted attachments, will now be attached and counted in the same manner as IMFRs. Affected documentation includes, but is not limited to—

- Approvals for Special Collection Techniques.
- ACIC Analytical Reports (for example, Link Analysis).
- Administrative messages that change the number of subjects or the name(s) of the SUBJECT(S), or that change an impersonal subject block to a personal one.
- CI special operations concept (CISOC) approvals.

- Federal Bureau of Investigation (FBI) Memorandums.
- SOI and responses to other SOIs from other agencies or commands.

CLASSIFICATION OF THE REPORT OF INVESTIGATION

E-98. **Marking.** Mark all paragraphs and subparagraphs in accordance with AR 380-5. Classify all subparagraphs based on content. Avoid over classification.

Note. Most record checks and interviews contain little or no actual classified information. Because of this fact, the ACICA generally declassifies all ROIs.

E-99. **Classification authority.** Carefully review the following references to determine which classification authority must be cited:

- AR 381-12.
- AR 381-47.
- INSCOM SCG 380-2.
- Supported unit classification guides/Special Access Program (SAP) classification guides.

E-100. Place the classification authority and the declassification instructions at the bottom of the first page. An example is shown below.

DERIVED FROM: Sec 2-2, Chapter 2
INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 2 DEC 96

E-101. **Caveats.** Use information-handling caveats as necessary on the ROI and in appropriate paragraphs. Mark all IMFRs, exhibit cover sheets, and exhibits with the appropriate classification. Apply common sense and familiarize all agents with current classification guidance. MULTIPLE SOURCES in the CLASSIFIED BY line should be listed individually at the bottom of page 1, unless there are so many that this becomes impractical. In such an event, a separate listing of the sources and their declassification instructions should be attached on a separate page.

Note. Bear in mind that most exhibits are NOT classified.

E-102. **Exhibits.** Ensure each exhibit has a completed exhibit cover sheet to accompany the exhibit. Double-check all classification markings (if needed). IMFRs written because of a polygraph examination that occurred as part of the investigation will report the findings of the examination and any critical comments as they pertain to the case. The DA Forms 2802 (Polygraph Examination Report) will not be attached as an exhibit.

REPORT OF INVESTIGATION LETTERS OF TRANSMITTAL

E-103. The ROI Letter of Transmittal prepared on appropriate letterhead will be signed by the Battalion Commander and addressed as shown in figure E-7. Figure E-8 (page E-52) provides an example of an ROI.

CLASSIFICATION (OF ROI)

IAMG-OP-ATCICA 30 November 2004

MEMORANDUM THRU Commander, 902d MI Group,
ATTN: IAMG-OP-ATCICA, 902d MI Group, Fort Meade, MD 20755

FOR Chief, Army CI Coordinating Authority,
ATTN: DAMI-CH-ATCICA, Fort Meade, MD 20755

SUBJECT: Letter of Transmittal Report of Investigation, CCN: 05-5555-902 (U)

1. (U) The Report of Investigation on ACICA CCN:05-5555-902; Reference, dated 25 November 2004,is enclosed for your action.

2. (U) My POC for this action is MAJ John Doe, Bn S-3, x77777.

Encl
as

JACOB P. ASTOR
LTC, MI
Commanding

DERIVED FROM: Sec 2-2, Chapter 2, INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 2 DEC 96

(Regrade Unclassified When Separated From Classified Enclosures)

CLASSIFICATION (OF ROI)

Figure E-7. Example of a transmittal letter for an ROI

CLASSIFICATION

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

IAMG-B-DT (381-20p) 21 AUGUST 2005

REPORT OF INVESTIGATION

1. (X) ADMINISTRATIVE DATA:

TITLE: JONES, John L.SPC, 000-00-0000 ACICA CCN: PI-BDT-03-019

DPOB: 20 Nov 82, Cleveland, OH

INVESTIGATING UNIT: 902D MI Group CONTROL OFFICE: ATCICA

DATE OPENED: 25 April 2005 DATE CLOSED:

REASON FOR INVESTIGATION: To determine if John L. JONES compromised classified information, and if the compromise involved espionage on behalf of a FISS and ITO entity.

CASE STATUS: Terminated

2. (U) SYNOPSIS:

SOURCE HAD NO OBJECTION TO HER NAME BEING RELEASED TO SUBJECT

INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM OFFICIAL GOVERNMENT RECORDS

DERIVED FROM: Sec 2-2, CH 2, INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 2 DEC 96

CLASSIFICATION

Figure E-8. Example of an ROI

CLASSIFICATION

IAMG-B-DT (381-20p) 21 AUGUST 2005

ACICA CCN: PI-BDT-03-019

THIS REPORT CONTAINS THIRD AGENCY INFORMATION WHICH WILL NOT BE DISSEMINATED WITHOUT PRIOR APPROVAL.

a. (X) In March 2005, SUBJECT may have removed a CD ROM containing classified information from HIS Reserve Unit, and placed the information on HIS home computer. Source, Karen R. Nesbith, SUBJECT's spouse at the time of the incident, reported that SUBJECT had a CD ROM in a tool box which HE had brought home from HIS reserve unit. Neither the plastic case in which the CD ROM was stored, nor the CD, contained any markings. When source asked SUBJECT about the CD ROM, HE indicated it was a government CD. Later that day SUBJECT became concerned as to the contents of the CD and inserted it into HIS computer. Source recalled seeing an eagle and some words in black near the bottom of the screen, but could not recall any of the words. Initially, She reported that the screen showed TOP SECRET markings on it, but then changed Her recollection to "classified," and then said it had some kind of markings indicating "not just anybody was allowed to access" the CD. (1, EXHIBIT I)

b. (U) On 15 May 2005 the Army CI Coordinating Authority conducted checks of the Defense Eligibility Dependent System and the Defense Clearance and Investigations Index. The Defense Clearance and Investigations Index check showed no record for SUBJECT. (2, 3)

c. (X) On 15 May 2005, interviews of personnel at SUBJECT's reserve unit revealed that SUBJECT did not display any CI indicators, the unit did not have any classified information on a CD ROM, and SUBJECT did not have access to classified information. Additionally, in approximately March-April 2005 timeframe, SUBJECT had quit attending weekend drills and the unit submitted paperwork to process SUBJECT out of the reserve program. (4)

CLASSIFICATION

Figure E-8. Example of an ROI (continued)

CLASSIFICATION

d. (X) During May-June 2005, the Cleveland, OH Federal Bureau of Investigation (FBI) office attempted to locate SUBJECT to conduct a joint FBI/US Army Intelligence interview. However, all efforts to locate SUBJECT were unsuccessful. ACICA suspended the investigation on July 5, 2003. On 1 August 2005, the FBI located SUBJECT and conducted an interview. SUBJECT denied any access to or compromise of classified information. SUBJECT, who was in a failing marriage, told source the CD Rom contained classified information; HE thought that would make HIM look important, and source would want to stay married to HIM. (5)

3. (X) CASE TERMINATED: This preliminary inquiry did not reveal any evidence of a security compromise, or espionage involvement by SUBJECT.

4. (U) ROI prepared by Special Agent Bill Bonn, A Company, 308th MI Battalion, 902d MI Group, Detroit Resident Office, Warren, MI 48397.

Encl
5 IMFRs
1. Exhibit

JAMES J. MONK
CPT, MI
Commanding

CLASSIFICATION

Figure E-8. Example of an ROI (continued)

SUMMARY OF INFORMATION

E-104. Figure E-9 is an example of an SOI.

CLASSIFICATION

DEPARTMENT OF THE ARMY
_____ Field Office
307th Military Intelligence Battalion
Fort Huachuca, Arizona 85613-7002

March 28, 1999

Special Agent David L. Bowie
Federal Bureau of Investigation Legal Attaché

Dear Special Agent Bowie:

Enclosed is a two-page Summary of Information (SOI), regarding an incident on a US Military Training Mission installation involving a foreign military officer.
Because the foreign national identified in the SOI is not subject to the investigative jurisdiction of US Army Intelligence, the details of the referenced incident are forwarded to your agency for any investigative action you deem appropriate.

This organization is willing to assist your agency (consistent with applicable regulations) in any inquiry/investigation you undertake, regarding this incident/individual, upon your request.
Point of contact is Special Agent William Raven, DSN 318-438-5555.

Sincerely,

Enclosure

WYATT B. ERPP
Special Agent in Charge
_____Field Office

DERIVED FROM: Sec 2-2, Chapter 2, INSCOM SCG 380-2
DECLASSIFY ON: Source Marked X1
DATE OF SOURCE: 2 DEC 96

CLASSIFICATION

Figure E-9. Example of an SOI

CLASSIFICATION

SUMMARY OF INFORMATION

PREPARING OFFICE: _____, 307th Military Intelligence Brigade
DATE PREPARED: 28 March 1999
SUBJECT: SCHMIDT, Helmut
CPT, German Army
DPOB: 3 May 1960, Suhl, GE (X//XX)
ACICA CCN: 98-0500-513

SOURCE WAS GIVEN AN EXPRESS PROMISE OF CONFIDENTIALITY AS A CONDITION FOR PROVIDING THE INFORMATION IN THIS SUMMARY.

1. (X//XX) On 26 March 1999, a confidential source reported the following information regarding Helmut SCHMIDT, CPT, DPOB: 30 November 1980, Berlin, Germany, Missile Leader, German Defense Forces hereinafter referred to as SUBJECT, who was an exchange officer at the HAWK Missile Repair Course, US Military Training Mission, Riyadh, Saudi Arabia:

a. (X//XX) On 25 March 1999, during a break outside the classroom, SUBJECT was overheard asking an unidentified US Army Captain for information regarding the US Army Brilliant Anti-Armor Sub-Munition. When the US Army Captain responded that Brilliant Antiwar Technology (BAT) information was not authorized for release to foreign military personnel, SUBJECT stated that HIS government would be willing to pay for information.

b. (X//XX) Source recalled that on 23 March 1999, He observed SUBJECT placing what appeared to be US defense contractor BAT advertisement brochures into HIS notebook. The brochures were not classified.

2. (X//XX) A check with the Command Security Manager and the Command Foreign Disclosure Officer disclosed that the BAT contains US Army missile technology classified SECRET and that the BAT is not approved for sale or transfer to any foreign country. The check also disclosed that no foreign personnel are accredited to the BAT program. The prime contractor for the BAT is XYZ Corporation, 1000 Memorial Parkway, Huntsville, Alabama.

3. (FOUO) A check with the US Commander of Military Training Mission Riyadh, confirmed SUBJECT's student status at the HAWK Missile Repair Course. SUBJECT has been assigned to Military Training Mission since 5 January 1999, and is scheduled to depart Riyadh on 15 April 1999, upon graduation from the course.

4. (U) A check of the local US Army CI cross-reference database disclosed no information regarding SUBJECT.

5. (X//XX) The source of information is Smith, Don; CPT; 425-12-1111; DPOB: 14 January 2007, Tucson, Arizona; Liaison Officer, US Military Training Mission, Riyadh, Saudi Arabia.

WYATT B. ERPP
Special Agent in Charge
_____ Field Office

CLASSIFICATION

Figure E-9. Example of an SOI (continued)

E-105. The Privacy Act of 1974 advisement statement is shown in figure E-10.

PRIVACY ACT OF 1974

ADVISEMENT STATEMENT

United States Army Intelligence is conducting an investigation of a CI matter pursuant to Army Regulations, which necessitates obtaining personal information from you. The Privacy Act of 1974 requires that each individual asked to provide personal information be advised of the following four points:

a. AUTHORITY: The Department of the Army is authorized to conduct CI investigations under EO 10450, "Security Requirements for Government Employees," EO 12333 "United States Intelligence Activities," and Title 10 of USC § 3012.

b. PRINCIPAL PURPOSES: This investigation is being conducted by the Army to permit responsible official(s) to determine the nature and extent of action, if any, necessary to ensure the security of the Army. The principle objectives in collecting this information are:

(1) To acquire factual information and/or evidence pertinent to the matter under investigation.
(2) To determine facts concerning possible compromise of US National Defense information.

c. ROUTINE USES: The information obtained from you will become part of Army records and will be provided to those officials responsible for the security of the Army. The information may, at Army initiative or upon request, be furnished to accredited Department of Defense activities, other Federal agencies, and/or to LEAs for their official use. Under certain circumstances, pursuant to applicable international agreements, the information may be provided to security and/or law enforcement officials of a foreign government.

d. VOLUNTARY OR MANDATORY NATURE OF DISCLOSURE: The disclosure of personal information is voluntary. However, failure to disclose necessary and relevant information which impedes the investigation may have an adverse impact on your security clearance, if you possess one, or are being considered for one, or your employment, if you are a military member or employee of the Department of the Army.

_____ (Date)

_____ (Signature)

Figure E-10. Privacy Act of 1974 advisement statement

E-106. The Perjury Warning is shown in figure E-11.

PERJURY WARNING

Under the provisions of Title 18, U.S. Code, Section 1001, whoever knowingly and willfully falsifies, conceals, or covers up a material fact, or makes any materially false or fraudulent statement, shall be fined or imprisoned not more than 5 years, or both. I understand the provisions of Title 18, U.S. Code, Section 1001, as stated above.

_____	_____
(Printed Name)	**(Signature and Date)**

Figure E-11. Perjury warning

E-107. The secrecy affirmation statement is shown in figure E-12.

SECRECY AFFIRMATION STATEMENT

WARNING NOTICE: SENSITIVE SOURCES OR METHODS INVOLVED

I, _____, hereby affirm I have been informed that

(Insert source's First name, Middle initial and Last name)

disclosure of the nature, source(s), or the existence of the CI activity in which I am involved or of which I have knowledge is prohibited without the expressed approval of US Army Intelligence. I further certify that I have been briefed on my security responsibilities for the information which we have discussed, and that any unauthorized disclosure by me of any information imparted to me or otherwise acquired by me regarding this CI activity will be considered in violation of the Uniform Code of Military Justice and/or the US Espionage Laws as defined in Chapter 37, Title 18 of the US Code.

_____ _____

DATE (day/month/year) SIGNATURE

_____ _____

Printed Name of Witness Signature of Witness

WARNING NOTICE: SENSITIVE SOURCES OR METHODS INVOLVED

Figure E-12. Secrecy affirmation statement

This page intentionally left blank.

Appendix F

Predeployment and Mission Planning

This appendix addresses predeployment actions the counterintelligence (CI) leader must take to prepare for deployment. CI leaders must anticipate, identify, consider, and evaluate all potential threats. They must take advantage of enhanced information flow through hierarchical and nonhierarchical networks (computer, communications, and personnel). CI leaders need to be involved with the operational planning and orders production to ensure CI assets are employed early and utilized properly. Success as a leader rests upon being prepared for the mission. The guidelines in this appendix will help the team leader develop a focused preparation plan.

MISSION ANALYSIS

F-1. Mission analysis should be the first and most important step. Mission analysis begins upon notification and continues until departure. Good analysis ensures the right personnel and equipment deploy. The parent and supported units will do much of the mission analysis. CI leaders should obtain a copy of mission analysis products from higher echelons before starting their own analysis. They should ensure they have an understanding of the tasks to be performed, the purpose behind accomplishing those tasks, the supported commander's intent, and any restraints placed on your element.

F-2. This information will come in the operation order (OPORD) from the parent or supported unit operations officer (S-3) or, if the mission is already established, through coordination with the unit currently in theater. The notification of any deployment and the readiness status of the deploying element dictate the time line. But if time permits, CI leaders should—

- Update threat databases.
- Review available databases on assigned contingency areas.
- Review, update, and/or develop intelligence preparation of the battlefield (IPB) products.

F-3. During the predeployment phase a CI team can obtain mission background by accessing the Secure Internet Protocol Router Network (SIPRNET). Most operations have an established site where information can be pulled down and questions can be asked. A well-established operation will have more information available. Information on initial entry situations will be more difficult to find and may have to be researched. The following are some types of information that should be collected and analyzed before a unit deploys:

- **Country studies.** Country studies will provide background on the country and people. This document will give you a better understanding of the environment. The CI team needs to look for a country study that presents both the historical and current situation. This will tell the team how far the country has fallen and will provide insight into dealings with the people.
- **Road to war.** The Road to War will focus on what led up to the conflict and the conflict itself. Knowing the reasons behind the conflict is important to understanding the people and interacting with them.

- **Current reporting.** Current CI reporting will focus the team on what is currently happening in country, establish what the collection priorities are, and give the team examples of how to write their reports.
- **Standing operating procedures (SOPs).** The unit's tactical standing operating procedures will further define the mission, equipment, and team requirements. All SOPs vary and when the team deploys it might not use its own SOP. For this reason, the team should conduct a review of the supported unit's SOP to ensure compliance.

PREDEPLOYMENT CONSIDERATIONS

F-4. **Predeployment integration planning.** CI operational activities should be integrated into established unit and higher echelon or headquarters operation plans (OPLANs). This integration should include information and reporting architectures, technical control and oversight for subordinate teams, responsibilities and function of operational management elements (staff2X, CI Coordinating Authority [CICA] and operational management teams [OMTs]), and financial management annexes for any source operations; for example, source operations and host country liaison.

F-5. **Information exchange.** Continuous contact with theater CI elements to facilitate information exchange will allow the CI team and operational management elements to become knowledgeable concerning the operational environment, previous reporting, current operational procedures, personalities, host-nation (HN) capabilities, and cultural nuances that CI elements will be required to understand to successfully operate and support the commander.

F-6. **Establish standing operating procedures.** The CI team should have pre-established plans and SOPs which vary according to the type of military operation.

F-7. **Operational integration.** Operational coordination and the covering agent program (CAP) to conduct liaison with supported units during predeployment exercises is vital. Liaison must be conducted with commanders, S-2s, administrative support personnel, logistical support personnel, communications personnel, and others. CI teams supporting specific units should obtain their supported unit's briefing slide formats, unit SOPs, and ensure all team members are aware of the procedures governing CI interface. This will allow the CI team to integrate into the supported unit's pre-mission planning and build trust and confidence with the supported command by exhibiting a habitual relationship between the supported unit's mission and the CI team. CI leaders should—

- Conduct liaison and coordination meetings (predeployment through redeployment) with representatives from other law enforcement, security and intelligence Army, Department of Defense (DOD), and U.S. national agencies essential to developing an all-source picture and to identify information gaps that may be satisfied by the CI team.
- Conduct 24-hour operations: automation, communications capacity, and personnel necessary to provide continuous intelligence information collection and requirements management, processing, and reporting.
- Plan and coordinate for linguistic support.
- Develop and forward requests for information (RFIs) to higher headquarters in accordance with SOPs to obtain all information required to complete predeployment and operational planning.
- Ensure that team data processing equipment is interoperable with the supported unit's network structure and appropriate interfaces are available.
- Ensure the CI team and operational management elements are integrated with supported unit exercises and mission readiness rehearsals to validate CI deployment information and reporting architectures, SOPs, load plans, and packing lists.

F-8. **Joint operations environment.** Organizations like the Strategic CI Detachment (SCID) in Multinational Force–Iraq (MNF-I) and Combined Forces Command–Afghanistan (CFC-A) will be more common and will reside on the joint manning document. Each service requires its CI personnel to follow the service-specific procedures even when working in a joint environment. Each service has a different way of doing things and varying degrees of restrictions, with the Army being the most restrictive.

F-9. **Freedom of movement.** CI teams work best in single vehicles or pairs rather than large vehicle convoys when the threat level is high. A low profile patrol is preferable to a show of force. Vehicles should have no markings, which can serve to identify the teams as MI (for example, bumper markings). The commander may approve the modification of MI unit vehicles to reflect that of the supported command. Likewise, the commander may agree to change the unit shoulder patch of the supporting MI Soldiers to that of the supported command. The 2X should pursue such initiatives.

F-10. **External CI teams.** Commanders will often see or hear of CI entities working in their area of operations (AO), which are not under their direct command. The tendency is for commanders to insist on either their removal or their assurance that they report to local commanders before operating in the area. These teams will be collecting for other agencies and formations and will therefore have different SOPs or priority intelligence requirements (PIRs). It will usually be unacceptable for reasons of security or unworkable for teams to check in every time they enter the AO. Commanders must accept that these teams or individuals cannot be controlled by subordinate commanders. Deconfliction, command, control, and communications (C3), cooperation, patience, and understanding all play an important part in resolving these situations. The 2X is the key to diffusing and resolving such situations.

F-11. **Protection and operational risk mitigation.** Commanders must weigh risk versus gain when considering protection measures for CI. Commanders may approve lower protection measures for teams on a case-by-case basis. Experience has shown that in non-hostile environments teams will be more successful when dressed in minimal protective equipment and unencumbered by crew-served weapons and rifles. In some situations, "dressing down" without badges of rank, unit designation, and ballistic protection will enhance operators' ability to gain rapport with sources rather than to intimidate them. Collectors will attempt, where possible, to appear the same as their maneuver colleagues. However, due to the very nature of their role, they may often appear to operate in very different ways.

F-12. **Communications.** Where possible, all teams should be in regular communications with their parent operations room or task force tactical operations center (TOC). However, recent operations have shown that this is not always practical nor possible. Tactical satellite radios have assisted in some cases; however, where this system is not available, commanders and staff must again weigh risk versus gain.

F-13. **Curfews and prohibited activities.** Frequently, teams will need to take part in activities prohibited to other Soldiers (for example, consumption of alcohol, remaining out past curfew, working in civilian clothes). Such exceptions must be used with discretion and approved, in advance, by the C/J/G/S-2 or 2X and appropriate commander.

F-14. **Incentive program.** Teams will have discretionary funds and incentive items to reimburse or entice sources and contacts. These items are subject to strict command discipline and accounting.

F-15. **Accommodations.** Mission requirements and operations tempo of the CI team should be considered when identifying a location for team operations and billeting. The optimal accommodations for a CI team within a compound are to be billeted in the same building or tent as their base of operations. This accommodation will allow the team leader to effectively execute mission requirements and develop an adequate sleep plan.

F-16. **Base of operations considerations.** Operations security OPSEC should be paramount when identifying a location for CI team base of operations. The CI team will routinely bring local national civilians onto the compound or base camp during the conduct of overt and discreet source operations, and to screen local civilians who are seeking employment. These operations dictate the need to locate the base of operations in an area of the compound that will reduce the local national civilian's ability to view

equipment, personnel, and activities. Additionally, discreet source operations require the base of operations to be located in an area conducive to the quick and discreet movement of sources on and off the compound.

F-17. **Billeting considerations.** The ability to billet the entire CI team together will produce a cohesive team, able to respond quickly to time-sensitive tasking during all hours. Additionally, CI operations are fluid in their execution and require team members to work unusual and unscheduled hours. Thus, the sleep plan and impact upon non-CI Soldiers are two critical considerations in billeting arrangements.

APPENDIX 3 (COUNTERINTELLIGENCE) TO ANNEX B (INTELLIGENCE) TO OPERATION ORDER

F-18. The intelligence staff prepares the intelligence annex of the operation order (OPORD). Annex B (Intelligence) of the OPORD, implements the command's intelligence plan. Each organization within the division uses the annex to understand how that the intelligence effort supports its operation. Appendix 3 (Counterintelligence) is the counterintelligence section Annex B (Intelligence). Figure F-1 is Appendix 3 (Counterintelligence) to Annex B (Intelligence) to an OPORD.

APPENDIX 3 (COUNTERINTELLIGENCE) TO ANNEX B (INTELLIGENCE)

1. MISSION:

Identify the scope of the CI mission and the objectives associated with the conduct of those missions. For example, 519th MI BN CI Teams will conduct CI Force Protection Source Operations (CFSO) to identify, counter, neutralize, or exploit the foreign intelligence and security services (FISS) and international terrorist organizations (ITO) intelligence threat targeting U.S./coalition forces. The 519th MI Battalion CI teams will conduct locally employed persons (LEPs) screening to asses host nation, indigenous, or third-country national persons for suitability to work for and have access to U.S. installations and facilities and identify potential threats to U.S./coalition forces. The mission statement should include all aspects of the CI mission; however, they should be discussed in broad supporting terms. Individual missions (for example, CFSO, LEP Screening, CI Investigations) should be detailed in separate Tabs supporting this appendix.

2. SITUATION:

a. FISS and ITO. Identify all known or suspected FISS and ITO elements within the CI element's area of intelligence responsibility (area of intelligence responsibility). This should include a summary of information on their capabilities, affiliations with other FISS and ITO entities, key personalities, methods of operation, and targeting focus b. Friendly. Identify all Army, DOD service, U.S. and coalition agencies and elements with the CI element's area of intelligence responsibility which may be leveraged for information or required for operational coordination purposes.

b. Friendly. Identify all Army, DOD service, U.S. and coalition agencies and elements with the CI element's area of intelligence responsibility which may be leveraged for information or required for operational coordination purposes.

c. Assumptions. List any assumptions that must be addressed to identify the operational execution and effectiveness of supporting CI elements. This may include command and support relationships, logistical issues (for example, supplies, equipment, and facilities), information reporting, and areas of operation (AOs).

Figure F-1. Appendix 3 (CI) to Annex B (Intelligence) to an OPORD

3. EXECUTION:

a. Concept of Operations. You must outline the concept of operations in as much detail as possible to ensure that all contingencies are covered. Be open to suggestions and recommendation even if they are just used as alternative courses of action (COAs) or branches off existing COAs.

b. The following priority tasks will be performed by CI assets. List exactly who you expect to be responsible for specific tasks down to company and team level, especially if you have specialized technical CI assets available. Consider how movement from phase to phase within the major operations battles and engagements will impact priorities, requirements, and missions and who will be available to execute the prescribed tasks.

(1) Phase I.

(2) Phase II.

(3) Phase III.

(4) Phase IV.

(5) Phase V.

c. Tasks.

(1) Parent Unit.

(2) Theater CI Coordinating Authority (TCICA).

(3) CI Coordinating Authority (CICA).

(4) Service components.

(5) Coalition CI assets and coordination.

(6) Brigade level asset coordination.

d. CI Collection and Reporting.

(1) C/J-2 retains Collection Requirements Management authority over all CI assets. Coordinate with the analysis and control element (ACE).

(2) CI assets will be tasked to fulfill CI collection requirements reflected in the CI Collection Plan produced to support this OPLAN. Make sure you have contributed meaningful input to the CI Collection Plan or you will not have any decent missions preplanned for you elements.

(3) Coordinate the release of national level CI reports through the CI Staff Officer (CISO) and/or the TFCICA before release. All national level products will be reported via intelligence information reports (IIR) format. All other CI reports will be in accordance with component regulations or unit SOPs. Upon or before execution of this OPLAN, C/J-2 will coordinate all other attached or assigned or operational control (OPCON) CI elements to ensure that unit SOPs are sufficient to provide continuity in CI reporting.

Figure F-1. Appendix 3 (CI) to Annex B (Intelligence) to an OPORD (continued)

(4) CI investigative reporting will be in accordance with AR 381-20.

e. CI Analysis and Production.

(1) The CISO will publish the initial CI threat assessment (CITA) to support this OPLAN. Subsequent CI analysis and production will be published by the CISO or his designated elements within the ACE and subordinate elements will perform analysis and production for dissemination within channels. Analytical products will be disseminated within the command and may be released to other consumers in accordance with established reporting guidance.

(2) The command will receive theater level terrorist warnings and advisories from the CISO. The ACE will advise the command on current threat information produced and collected locally. Additionally the ACE will produce analysis products of threat information received from higher-level collectors.

f. CI Investigations.

(1) The command will conduct CI-oriented investigations. The Army Theater CI Coordinating Authority (ATCICA) will provide technical control and oversight, in accordance with applicable regulations for all CI investigations within the AO. Commanders will be apprised of investigations on a strict need-to-know basis. The TCICA is the release and dissemination authority for all CI investigations occurring in the AO.

(2) CI elements involved in CI investigations will operate in accordance with all applicable Army and DOD regulations and directives.

(3) HN requirements for apprehension and/or detention of personnel involved, for example, in espionage, sabotage, will be disseminated through the TCICA when published by the CISO.

(4) Procedures for the conduct of other CI investigations will be published as necessary.

g. CI Operations.

(1) The CISO is responsible for the planning, coordination, and oversight of CI operations and activities within the AO.

(2) Consistent with requirements and priorities determined by the CISO and supporting commands, CI elements will develop CI target lists, collection requirements, and black (detain) white (protect), and gray (suspect) lists within the AO.

(3) CI elements will, with the C/J-1 and the local contracting office when applicable, conduct screening and vetting activities for locally employed persons (LEPs) to determine employability of the LEP before hiring.

(4) CI elements, in coordination with supporting Military Police organizations and theatre interrogation facilities, will conduct CI screening operations of refugees, displaced persons, enemy prisoners of war (EPWs), and detained suspects for CI exploitation.

Figure F-1. Appendix 3 (CI) to Annex B (Intelligence) to an OPORD (continued)

h. Coordinating Instructions.

(1) The CISO and TFCICA will be apprised of significant CI activities and operations.

(2) Intelligence Oversight. The J-2 will ensure all support CI activities and operations are conducted in accordance with all applicable regulations and directives.

(3) Intelligence Contingency Funds (ICF). ICF will be the responsibility of the subordinate CI elements and their respective commands.

4. SERVICE AND SUPPORT:

In accordance with annex I (Service Support), specific service and support needs will differ according to the tactical situation, mission, methods, and time line of deployment. List any unique intelligence service support (for example, contractor support) not addressed in either the base order or annex I.

a. Command-regulated classes of supply. Highlight subordinate allocations of command-regulated classes of supply that impact functional area operations (such as the controlled supply rate). Summarize in a matrix or table if necessary.

b. Supply distribution plan:

- State the method of supply (supply point or unit distribution) to be used for appropriate classes of supply for each subordinate or supporting unit.
- Give tentative locations for supply points or locations for linkup of push packages direct to units.
- Give allocation of classes of supply by subordinate unit, control measure, or combination. Summarize in a matrix or table, if necessary.

c. Transportation. State the allocation and priority of support of haul or airlift assets dedicated for moving classes of supply.

d. Health service support. Address arrangements made for health support of functional area units operating in forward maneuver unit areas.

e. Maintenance. State priority of support, locations of maintenance facilities, and any relevant policies.

f. Field services. State priority of support, locations of facilities, and command policies.

g. Host Nation:

- List type and location of HN functional area facilities, assets, or support.
- List procedures for requesting and acquiring HN functional area support.
- Highlight any limitations or restrictions on HN support.

5. COMMAND AND SIGNAL:

a. Command.

- State the location of key functional area leaders.
- Designate a functional area chain of command and succession of command.
- Designate a headquarters to control the effort within functional area work lines on an area basis.
- List command posts and other command and control facilities and their locations.

b. Signal. Address any functional-area-specific communications or digitization connectivity requirements or coordination necessary to meet functional responsibilities.

This page intentionally left blank.

Appendix G

Counterintelligence Support to Multinational Operations

Multinational operations, both those that include combat and those that do not, are conducted within the structure of an alliance or coalition.

MULTINATIONAL OPERATIONS

G-1. An alliance is a result of formal agreements between two or more countries to support broad, long-term objectives, usually involving mutual defense. North Atlantic Treaty Organization (NATO) is one example of an alliance. Alliance operations are synonymous with multinational operations.

G-2. A military coalition is an agreement between countries to commit military forces for a temporary period for some specific purpose. An example of such a coalition is the military force that restored Kuwaiti sovereignty in Operation DESERT STORM.

G-3. Multinational operations may involve a coalition, but be led by an alliance and rely upon the military structure of the alliance. An example of an alliance-led operation is the NATO-led peace enforcement mission in Bosnia-Herzegovina known as Stabilization Force.

G-4. Multinational CI is an integrated effort by two or more nations working together to support the CI requirements of a multinational force. It is a cooperative effort that provides mission-focused connectivity and unity of effort to multinational headquarters to support associated units, facilities, and personnel. Each contingency deployment will have unique CI support requirements that will impact both structure and operations. Multinational cooperative planning should begin at the earliest possible stages of a contingency deployment to maximize the multinational effort.

RATIONALE FOR MULTINATIONAL OPERATIONS

G-5. Protection is a paramount responsibility of command, regardless of nationality. Command responsibility includes an active CI effort, just as it would in any U.S. deployment.

- All combatant commanders have an protection mission. “Command” necessarily includes protecting the assigned and attached forces. CI may participate in multinational efforts either as a U.S.-only or a multinational CI element. CI support to multinational commands should be based on the concept of centralized control and decentralized execution. Multinational CI can range from very limited coordination between CI elements of participating nations to a fully integrated effort. The focus and level of coordination of multinational CI operations will be determined by the coalition intelligence directorate or the combined joint staff CI and human intelligence operations coordinator (CJ-2X), not by the nations themselves.
- Multinational commands should receive coordinated CI support from the participating military and national CI organizations other supporting agencies. In some multinational deployments, the United States will not comprise the predominate force, nor will it always be the most capable of executing the CI mission.
- Multinational CI effort should be developed early. If an alliance organization has an existing CI structure, it should be used as a foundation for deployment. In the case of the formation of a coalition, combined CI concepts should be considered to ensure their effective implementation before deployment. Planning for the functions of CI collection and production and dissemination would need to be formalized in standing operating procedures (SOPs).

CONCEPT OF MULTINATIONAL COUNTERINTELLIGENCE ACTIVITIES

G-6. Sharing of CI information is critical to the multinational commander's protection efforts and is critical to the multinational CI effort. CI support to multinational operations may include the following:

- Combined source registration, cross-coding, and methods to safeguard data.
- Protection support to nongovernmental organizations (NGOs).
- Intelligence processing, classification, and dissemination based on participant capability and need to know.
- Establishment of legal baseline between participating nations.
- Communications and automation architecture interoperability.

COORDINATION OF MULTINATIONAL COUNTERINTELLIGENCE ACTIVITIES

G-7. Coordination of CI effort at the multinational level is a requirement for an effective combined CI effort. Service CI components should leverage existing liaison relationships with other countries' services to strengthen CI support within the area of responsibility (AOR) or joint operation areas whenever possible. Unless there is a preponderance of combat forces from a single nation, future multinational efforts will require the participation of CI personnel from more than one nation. Proactive sharing of historical data and crisis-related information to ensure proper knowledge of the operational environment should be the standard for information sharing.

G-8. Such considerations should include the following:

- Appropriate security classification guides.
- Comprehensive pre-deployment threat data and appropriate CI training.
- Impact of cultural, political, and linguistic considerations on providing flexible CI protection.

G-9. There must be a clear understanding that the multinational environment is fluid and dynamic. Political considerations and military necessity make any hard-and-fast rules impractical. Consequently, all handling and dissemination procedures for United States originated classified information should be included in the contingency planning process by the senior U.S. CI representative supporting the geographic combatant commander. Additional factors concerning the relationship of multinational partners must be considered. Sensitive material may be released by one partner with the intention of vertical release only and not lateral dissemination to other multinational partners. Mechanisms must be developed for safeguarding sources from potential compromise.

G-10. Liaison with host-nation (HN) and multinational security and CI forces, United Nations forces, NGOs, and other entities may supports CI collection efforts. All of these agencies represent potential sources of information that may assist in protection directly and support other CI functions indirectly. When participating nations have their own CI units to support their own forces, liaison with these CI units is critical to serve the needs of multinational force commanders in their protection responsibility. The level and type of information to be shared and the means concerned must be addressed during pre-deployment planning.

RESPONSIBILITIES DURING MULTINATIONAL COUNTERINTELLIGENCE ACTIVITIES

G-11. It is the responsibility of the designated U.S. CICA or the senior U.S. intelligence officer to explore the potential and possibilities of conducting some form of multinational or joint CI to support the

multinational force commander. Such coordination should be effected by assigned CI personnel of the highest U.S. headquarters assigned to the multinational command if no CICA is designated.

G-12. The nature of the alliance or coalition, its mission, its expected duration, the nature of the threat, the degree of the participation by each nation, and the political situation are factors that bear on whether multinational CI should be attempted. Each nation will make its own decision to participate in multinational CI based on its own national interests.

G-13. Regardless of the nationality of the force commander, intelligence officer, or CICA, U.S. CI agents are subject to U.S. laws, regulations, and guidance when serving in a multinational environment. This must be identified early in the planning process, as these limitations will have a direct impact on the effectiveness of the overall organization.

G-14. Many nations do not have robustly developed concepts for CI support of combat forces in the field. Those that have a concept have many variations on how CI forces are organized.

G-15. In addition, the definition of the terminology of CI and security may vary extensively, so it is extremely important to verify the exact definitions early in the process.

MULTINATIONAL COUNTERINTELLIGENCE COLLECTION AND REPORTING

G-16. Participation in multinational CI offers a unique opportunity for liaison for collection with cooperating coalition or HN intelligence services. This closer contact thus contributes more significantly to the in-theater multinational force CI effort than that of a single nation.

G-17. CI requirements management should be the responsibility of the senior CI officer conducted with the commander's C/J/G/S-2 and the collection manager. The nationality of key intelligence personnel in the multinational force organizational structure may be a limiting factor.

G-18. CI teams must be equipped with compatible portable computers and secure communication equipment devices to rapidly communicate with the coalition senior CI officer.

G-19. Reports that relate to the execution of CI missions will be transmitted only via dedicated, secure communications. Reports that indicate imminent threat will be transmitted not only to the senior CI officer but also immediately to the threatened command over the most expeditious and practical means weighing information perishability with OPSEC.

G-20. Coordination requirements for source operations and other sensitive activities will be the subject of extensive negotiation between the participating nations, and subject to extensive legal review. It is important than CI operational concept is approved by the multinational force commander so that these very productive activities can be carried out in a timely manner.

MULTINATIONAL COUNTERINTELLIGENCE ANALYSIS AND PRODUCTION

G-21. Close liaison with military and civilian CI personnel of participating nations provides additional sources of information. In some cases, one nation may have better databases on information of CI interest than another nation.

G-22. The robustness of the multinational CI analysis and production effort will depend on the resources made available by participating nations.

G-23. Dissemination of critical CI information should be through secure communications available for the dissemination of intelligence traffic. Multinational commands could lack robust secure communications, and dedicated secure CI communications may be the only means for timely dissemination of critical threat information.

INVESTIGATIONS

G-24. If the subject of an investigation is known to be a citizen of one of the multinational force nations, that nation must be notified and may assume primary investigative jurisdiction. If the nationality of the subject is unknown, primary jurisdiction will remain with the multinational headquarters CI unit; however, primacy may change once nationality is determined.

G-25. When an investigation involves a member of the military components of NATO, the 650th MI Group will assume primacy and notify the concerned nations.

G-26. In either event, the multinational CI unit will support the investigative process and facilitate access to multinational force activities to further the investigation.

SHARING OF COUNTERINTELLIGENCE INFORMATION

G-27. Each nation will determine what CI information is in its national interest to share. Information may be provided to the senior CI officer with specific caveats for its protection; in all instances, these caveats must be respected if the exchange of information is expected to continue.

G-28. In general, most information collected during multinational CI activities will be released to the multinational command. This concept applies whether CI personnel are operating in a single-nation capacity or as part of a multinational CI effort. All information directly supporting or dealing with protection and multinational force security must be provided, at a minimum, to the multinational force commander, the C/J/G/S-2, and the senior CI officer.

G-29. The use of restrictive caveats should be kept to a minimum. The decision-making criteria should be "what not to release" vice "what to release."

G-30. CI information sharing needs to be in the spirit of the multinational effort with the focus on the protection mission. While it is expected that individuals from each nation will have access to the equivalent of "not releasable to foreign nationals" information, all should seek to get release to the multinational command that information which will assist in protecting the entire multinational force.

LIMITATIONS AND CHALLENGES

G-31. Unreliable alliance or coalition partners will negate the effectiveness of multinational CI. In some cases, the multinational CI effort may be carried by only one nation or a few member nations of the alliance or coalition. Some potential alliance or coalition partners may not have developed the necessary military doctrine for the employment of CI to support military forces in the field. Consequently, they may not have CI personnel in the military, or who can operate in a field environment. If CI personnel exist, they may not be adequately equipped to perform the mission.

G-32. Multinational commands should receive coordinated, combined CI support from the military and national level CI organizations and the combat support agencies of the nations participating. Since it is a multinational effort, the development of multinational CI constructs will usually be subject to a process of negotiation between the participating nations.

G-33. In some deployments, the United States will not be the predominate force, nor will it necessarily be the most capable or expert to execute the CI mission. In many cases, other nations will have a more solid basis for conducting CI operations due to their experience in the area, the language capabilities of their intelligence personnel, or because they may already have extensive experience in the area due to recent deployments.

G-34. Negotiations to achieve critical cooperation in the area of CI will require CI personnel to avoid parochial Service or nationally biased approaches and recognize the potential significant contribution to be made by CI personnel of all the participating nations to the security of the multinational command.

Appendix H

Automation, Communication, and Equipment

Modern automation and communications systems are vital to counterintelligence (CI) operations and activities. Real-time collaboration, detailed operational planning and intelligence, synchronization, and reconnaissance (ISR) integration, as well as enhanced collection and source exploitation tools, must support team efforts. Emerging technology continues to allow the entire CI system to operate more effectively. CI assets must have the best possible technology not only to enhance collection but also to optimize the survivability of the CI special agents. Commanders may not be able to rely solely on standard military equipment but must be prepared to bridge the inevitable technological development gaps through the technical insertion of commercial-off-the-shelf technology (COTS) or government-off-the-shelf technology products.

AUTOMATION

H-1. CI automation uses common hardware and software solutions with a flexible interactive user interface to provide standardization of equipment and processes across all operational environments and conditions. CI automation must be deployable, survivable, network ready, and scalable to fit the mission or force package. System components must be capable of intelligence reach to support forward-deployed elements. CI automation allows integration and interaction with existing intelligence operations and systems, CI operational systems, and national-to-tactical databases. This integration allows operations personnel and analysts to develop plans, levy collection and operational requirements and investigations, as well as to manage, control, analyze, and report the information collected. CI automation—

- Provides connectivity and reach capability across all echelons of CI activity.
- Receives higher echelon requirements and transmits requests for information.
- Allows for CI collaboration and information sharing with joint interagency and coalition task forces.
- Pushes requirements, requests, and plans for CI operations in theater as required.
- Maintains the central CI database for the theater or area of operations (AO).
- Leverages joint, theater, and national level requirements and products for strategic, operational, and tactical CI assets in theater.
- Enables CI to provide accurate and timely correlated information to supported commanders through established reporting channels.

DISTRIBUTED COMMON GROUND SYSTEM–ARMY

H-2. Distributed Common Ground System–Army (DCGS-A) is the Army's ground processing system for all ISR sensors. DCGS-A integrates existing and new ISR system hardware and software that produces a common net-centric, modular, multi-security, multi-intelligence, interoperable architecture. DCGS-A provides access to data across the Army intelligence enterprise as well as facilitates intelligence reach operations with knowledge centers.

H-3. DCGS-A provides access to Joint Worldwide Intelligence Communications System (JWICS), National Security Agency Network (NSANet), Secure Internet Protocol Router Network (SIPRNET), and

Nonsecure Internet Protocol Router Network (NIPRNET). DCGS-A links tactical ISR sensors along with weather, space, and geospatial analysis capabilities to the Army intelligence enterprise. The DCGS-A net-centric capability enhances distributed operations by allowing ISR data access down to tactical units. Additionally, it provides the analyst data mining, fusion, collaboration, and visualization tools to conduct situational awareness, ISR synchronization, targeting support, analysis, and reporting.

H-4. DCGS-A provides users access to ISR raw sensor data, reports, graphics, and web services through the DCGS-A integration backbone (DIB). The DIB creates the core framework for a distributed, net-centric intelligence enterprise architecture. The DIB enables DCGS-A to task, process, post, and use data from Army, joint, and national ISR sensors. The DIB provides a metadata catalog that defines how you describe data. The metadata allows DCGS-A to expose the required data elements to the user.

H-5. DCGS-A is the primary ISR processing system from the joint task force (JTF) down to battalion and below units. DCGS-A is the ISR component of the battle command system and provides the intelligence, weather, and geospatial engineering data to battle command. It provides threat reporting and the threat portion of the common operational picture, the publish and subscribe services for ABCS users, as well as accesses friendly unit information for DCGS-A users. DCGS-A provides the analyst data mining, fusion, collaboration, and visualization tools to quickly sort through large amounts of data to provide timely, relevant intelligence to the commander.

H-6. DCGS-A tools assist the targeting process as well as synchronize ISR collection. DCGS-A not only provides the analyst access to national and theater data sources but also serves as a ground station for organizational ISR sensors. DCGS-A facilitates distributed operations and reduces the forward physical footprint.

H-7. DCGS-A will eventually integrate all intelligence systems and applications into a single architecture including CI automated collection and reporting systems.

BIOMETRICS

H-8. CI teams may be equipped with portable equipment for collecting, storing, analyzing, and retrieving biometric information. A biometric tool set is able to identify personnel by identifying biometric characteristics of the individuals. A database links identifying characteristics with all previous reports related to the person. Once a person's identifying baseline characteristics are entered into the database, if that person is again detained and scanned, the system has a probability of identifying them that approaches 100 percent accuracy.

H-9. The hardware that makes up a biometric system often consists of COTS in semihardened laptop computer running an operating system with a graphical user interface. It has a camera and an iris scanner, each of which is portable and can be used independent of the computer to collect and temporarily store information. The system also includes a fingerprint scanner that conforms to Federal Bureau of Investigation (FBI) requirements for admissible evidence. The fingerprint scanner must be attached to the computer during use.

MACHINE TRANSLATION AND INTERPRETATION

H-10. Understanding oral and written communication in a foreign language is often critical in CI activities and operations. The optimal solution is to have an individual who is a trained collector of native proficiency, totally versed in the local situation and U.S. requirements, has a requisite security clearance, and is capable of reporting accurately in English.

H-11. A commander's access to such individuals is sometimes problematic. This requirement is met through a combination of MI linguists, native speakers within the Department of Defense (DOD) system, and locally hired civilian translators. Difficulties arise if the proficiency levels of MI linguists are not up to mission requirements, or if the linguists do not possess the proper language for the theater of operation. Using locally hired translators raises security problems. In light of these conditions, an increasingly viable solution for the commander is the use of machine translation devices to meet some of these requirements.

H-12. Voice and text translation machines or software are critical in augmenting available linguists. This includes natural language processing, artificial intelligence, and optical-character recognition (OCR) capabilities. The basic application of machine translation, such as speech recognition and OCRs, dramatically increases the speed of processing information. Software programs are becoming widely available that allow a non-linguist to determine the intelligence significance of a foreign document, aid linguists with laborious tasks, and add consistency to human translation.

H-13. Machine interpretation is the use of a machine to interpret the spoken word between the CI special agent and another individual speaking a foreign language. Linguists are in high demand during operations and usually limited in number. As machine interpretation devices that address this problem become available to the field, they will improve the communication ability of non-linguists.

AUTOMATED ANALYTICAL TOOLS

H-14. The requirement for a robust CI single-discipline analytical capability extends through all echelons from national level to the operational management teams (OMTs). Communication between CI analysts at the operational level and analysts at the staff level may best be accomplished through a web-based communication capability. Web-based visual analytical tools allow maximum analyst participation in the development of products geared to mission planning, targeting, and information analysis at all echelons. Analytical products must be responsive to the special needs of a specific collection operation, project, or element.

H-15. CI special agents run operations in terrain consisting of persons, organizations, and installations of interest. Intelligence analysis support determines the specific terrain in each team area and how it differs from one team's named area of interest (NAI) to another. Specific products include studies on nominated targets (persons, organizations, and installations) and trends based on CI reporting, as appropriate, and visual analysis products (time event charts, matrices, link analysis diagrams, and organizational diagrams).

H-16. Automated CI analytical tools (such as time event charts, association matrices, activity matrices, and link analysis diagrams) improve predictive analysis capability. They save time and permit access to more complete information thus producing a more accurate, timely product.

H-17. Automated analytic techniques, aided by computerized virtual-viewing programs, allow the analyst better visualization of the operational environment. These programs assist the analyst in developing predictions and identifying information gaps to support targeting and collection. Automation and web-based tools allow the analyst to—

- Track and cross-cue CI reports.
- Incorporate data extraction technology, retrieval, automated data organization, content analysis, and visualization.
- Share analytical decisions with CI teams and other analysts in real time.
- Apply multidimensional technologies, content analysis techniques, and web-based collaborations.
- Display analytical results and view CI operations in real time.
- Share resources such as models, queries, visualizations, map overlays, and tool outputs through a common interface.
- Apply clustering (a nonlinear search that compiles the results based on search parameters) and rapid spatial graphical and geographic visualization tools to determine the meaning of large informational streams.
- Rapidly discover links, patterns, relationships, and trends in text to use in predictive analysis.
- Capture analytical conclusions and automatically transfer to intelligence databases and systems.

SEARCH ENGINES

H-18. Search engines provide access to previously collected or known information facilitating the development of comprehensive analytical and intelligence products and avoiding unnecessary collection tasking redundancy. A tool set for data visualization, search, and discovery is required, which is embedded with several software programs for manipulating data from multiple databases.

H-19. The types of modules in visualization packages should include search engines and knowledge discovery (semantic clustering) for unformatted data, applications for extracting and organizing formatted data, and data labeling. The package should also include a model building tool to enable users to make their archives more efficient with respect to search, retrieval, and compatibility to other applications as well as archiving and maintenance tools to support what will eventually become a large data warehouse. Search engines should be—

- Multilingual and able to query multiple classified and unclassified databases.
- Capable of developing, querying, and manipulating stored information.

WEB-BASED REPORTING

H-20. Web-based reporting employs current Internet technology. It employs an interactive graphic interface using client browser technology, search engines, hyperlinks, and intelligent software agents for searching, finding, viewing, and maintaining databases and supporting CI work, data, and information flows. It supports collaborative analysis at multiple echelons through connectivity on the SIPRNET. The following pertains to web-based reporting:

- Web-based databases compatible with any computer hardware, operating system, or software.
- Firewalls and information access which are controlled at each level with an approving systems administrator at each level conducting quality control through release authority procedures.
- Graphic user interface which uses standard Army and DOD report formats.
- Graphic user interface which walks the user through a critical task and is able to identify Army and DOD reports as required. Reports must be Army and DOD platform compatible and transferable through and to their respective systems.
- Multimedia supports applications for attaching, associating, and hyper linking video, still photographs, voice, scanned objects, graphics, and maps to records and files.

H-21. Web-based reporting and web pages developed for specific products allow the user to—

- Leverage their effort and expertise against all requirements, not just the ones that must be met immediately.
- Identify timely intelligence gaps and the leads to fill those gaps.
- Ensure immediate analytical feedback on collector reports to—
  - Post questions directly to a web page to enable all CI teams to answer or be cued to the specific request.
  - Identify or request clarification on questionable data for quality control.
- Fuse CI information and all-source information as required.
- Focus collection teams supporting maneuver commanders' requirements more effectively.
- Immediately extract information for crisis reaction.

DATABASES

H-22. Without databases, information is difficult or impossible to retrieve quickly, especially under adverse conditions. Databases support many complex CI functions and requirements, including—

- Mission deconfliction.
- ISR synchronization.
- Requests for information (RFIs).
- CI analysis.
- Summary, report, and assessment preparation.
- Threat and friendly situations tracking.
- Targeting.

H-23. Databases interact with other tools to support predictive analysis, prepare graphic analytical products, and provide situational awareness down to the CI team. These databases—

- Support time event charts, association matrices, support link analyses, and other analysis tools.
- Require a designated systems administrator at each. To ensure a high degree of integrity, discrepancies must be verified for accuracy.
- Allow operators, managers, and analysts to—
  - Compartment (protect) source-sensitive operational database segments, files, records, and fields.
  - Create, update, and maintain databases from locally generated information.
  - Import complete or partial databases from larger or peer databases.
  - Export complete or partial databases to peer or larger databases.
  - Share databases between peers, subordinates, or higher with appropriate access authorization.
- Provide systematic processing and automated parsing using standardized forms in intelligence operations, which are automatically parsed into appropriate databases for information storing, sharing, retrieval, and analysis.
- Allow query functions for decisionmaking as well as operational and analytical support.
- Provide analytical programs able to correlate data that facilitate information retrieval from any data repository.
- Incorporate information retrieval functions such as browsing (that is, point and click), key word searching, concepts, and similar functions.
- Support a suite of specialized decision support software—a set of tools which supports CI source administration, analysis, and risk management decisions. Decision support software tools should produce a set of CI reports specifically tailored to the CI decisionmaking, analysis, and assessment process.

2X AND CICA REQUIREMENTS

H-24. The counterintelligence (CI) automation systems are normally shared systems used by both the CI and human intelligence (HUMINT) communities. They must allow for network centric operations. The CI staff elements require the capability to send and receive data between subordinate OMTs and CI teams as

well as data exchange between higher and adjacent echelons. Automation requirements for the staff CI and HUMINT operations coordinator (2X)/CI Coordinating Authority (CICA) must be able to support CI mission planning, reporting, and dissemination. Their systems must also be interoperable with other service systems and automated analysis systems, manipulate CI databases, conduct reach, and have access to CI analytical tools.

OMT AND CI TEAM LEADER REQUIREMENTS

H-25. The OMT must be able to track teams and team members; receive and transmit data including graphic data to and from higher, lateral, and lower CI elements; create, receive, edit, and transmit reports; conduct single-discipline CI analysis; receive and transmit technical support information and tasking information; conduct reach; and conduct mission planning.

INDIVIDUAL COLLECTOR AUTOMATION REQUIREMENTS

H-26. The key to effective CI collection is unimpeded communication between the collector and the source of information. Any technological support to CI collection must be as unobtrusive as possible to minimize the intimidation factor when dealing with human sources. The individual collector must be able to—

- Record (both video and voice) conversations with sources.
- Scan, translate, and transmit documents and photographs.
- Instantaneously locate themselves in both rural and urban environments.
- Immediately access local, theater, and even national level databases.
- Communicate instantaneously with other team elements.

COUNTERINTELLIGENCE WORKSTATION REQUIREMENTS

H-27. CI teams have organic computer and data processing equipment. These workstations provide CI teams with productivity and management and analysis tools. They also provide SIPRNET connectivity and processing capability to identify requirements and facilitate reporting into other DOD systems as required. Included software graphically uses standard Army, DOD, and CI reporting, symbols, and map overlay generation and map plotting. Teams use workstations to—

- Provide quality control and dissemination of reports from the subordinate CI teams.
- Direct activities of subordinate CI teams and provide management to them.
- Perform single-discipline CI analysis for the supported commander.
- Transmit intelligence and administrative reports in near real time to higher headquarters.
- Receive tasking and administrative reports from higher headquarters and distribute to CI teams as required.
- Consolidate local databases and provide database input to higher headquarters.
- Receive database and digital information from higher headquarters and pass to lower and vice versa.

COMMUNICATIONS

H-28. Successful CI activities and operations must be supported by multiechelon technical oversight and a communications system that provides internal team communications linking CI teams to OMTs, and OMTs to higher headquarters, analytical elements, and theater and national agencies.

COMMUNICATIONS ARCHITECTURE

H-29. The CI collection architecture requires access to several communications and processing nets. These nets provide the framework needed to coordinate the tasking, reporting, command and control (C2), and service support of CI collection units spread across the width and depth of the operational environment. Under most operational scenarios, CI teams are not stationary. They are constantly moving throughout their supported command's AO and are able to communicate on the move. They cannot rely on fixed communications nodes for support.

H-30. Communications redundancy ensures that the loss of any one system does not severely disrupt CI operations. CI teams and OMTs normally operate at the collateral security level to ensure the timely dissemination of combat information and targeting data to organizations operating outside MI channels. The C/J/G/S-2X normally requires access to top secret (TS) communications capabilities to maintain coordination with national level agencies.

H-31. The CI collection assets use three basic communications nets: the operations and intelligence net, a command net, and a CI-specific technical net. Dependent on their mission and the operational environment location, the CI teams may also need to monitor the fire support element, aviation, or air defense artillery (ADA) communications nets.

- The operations and intelligence net links the collectors and producers of intelligence to the consumers of the intelligence information. It is used to pass information of immediate value to the affected unit and to analytical elements at the supported unit.
- The command nets exist at every echelon of command. They link the superior headquarters with its subordinate elements. Normally a unit will operate on two command nets; the one that links that unit to its higher headquarters and the one that links that unit to its subordinate elements. CI elements will also use their unit's command net to coordinate logistic and administrative support.
- The CI-specific technical nets link the control team to all of their subordinate collection teams and to the centers or organizations that provide the databases and technical guidance necessary for single-discipline collection and analysis. For example, the technical net would connect CI teams through their control teams to the S-2X and higher echelon CI analysis organizations.

COMMUNICATIONS REQUIREMENTS

H-32. CI communications requirements vary with each element's mission and location as follows:

- Individual CI collectors must maintain communications capability with the other team members and the team leader while dismounted. CI special agents, especially when supporting offensive and defensive operations, may be deployed as individuals. They need to maintain contact with their team leader for technical and operational support.
- The CI team needs to coordinate with the staff to operate anywhere within the supported unit's AO. They may operate mounted or dismounted. If supporting airmobile, airborne, amphibious, or other mobile operations, they may not have access to their vehicle-mounted communications systems for the critical early stages of these operations. They receive and report operational and technical information, as well as report intelligence information to the OMT using their unit's command net. They monitor their superior unit's operations and intelligence net. If in direct support (DS) to a maneuver element, they also monitor the command net of the unit they are supporting.
- OMTs normally operate on the superior unit operations and intelligence net, their unit C2 net, and the CI technical net. If the OMT is in DS, it must also operate on the C2 net of the supported unit.

- The C/J/G/S-2X operates on the C2 net, monitors the operations and intelligence net and controls their echelon CI technical net. The 2X needs secure (TS) communications capability to coordinate operations and pass data between themselves and higher CI organizations.

RECOMMENDED EQUIPMENT LIST FOR CI TEAM OPERATIONS

H-33. This materiel and equipment list is provided as a sample of what a CI team may require to support the commander's critical information requirements (CCIRs). Some of the equipment that is intended to be given to a source should be considered expendable. This kit assumes a four-person configuration for each echelon. Regardless of support relationship (organic, DS, general support [GS], general support-reinforcing [GSR]), CI teams inherently require the following:

- Survivability and security:
  - Two M1114 armored high-mobility multipurpose wheeled vehicles (HMMWVs).
  - One crew- or squad-served weapon per team, mounted and dismountable.
  - One M16A2 per team.
  - Three M4s per team.
  - Four 9mms per team.
  - M68 Aim-point System.
  - Appropriate body armor with specified ballistic armor protection for each team member.
- Collection and reporting system. Some of this equipment is also intended for source use and therefore should be considered expendable.
  - Baseline system.
  - Laptop.
  - Two hard drives (nonsecure Internet protocol router and secure Internet protocol).
  - Biometrics.
  - Camera equipment.
  - Printer.
  - Accessories (plugs, universal serial bus [USB] hub, Global Positioning System [GPS]).
  - Specialty kits:
    - Computer forensics equipment (first responder kit, SIM card reader).
    - Document and media exploitation (DOMEX) or machine-language translation equipment.
    - Desktop accessories.
    - Kit Bag-related items.
    - Forensics (computer and electronic media).
    - Communications kit.
    - Specialized surveillance or source issue (team) equipment.
  - Software:
    - Source Management Tool.
    - Link Analysis (Analyst Notebook).

  - Mapping—Single, standardized tool (down to 1:12,500 scale maps, operational graphics, GPS interface).
  - Biometrics Integration or Biometrics Enrollment Tools (Integrated Automated Fingerprint Identification System) compliant 10-print fingerprint scanners, iris scanners, photographing station).
  - Basic DOMEX application.
  - Foreign Language Machine Translation and Interpretation capability.
  - Mission Planning Software.
  - Query Tools: basic, advanced, multi-entity, multi-media, save user-defined queries.
- Peripherals 1 × CI team:
  - Digital video or still.
  - Digital voice recorder (USB interface).
  - Communications—requires organic communications systems to higher and laterally (non-line of sight and line of sight).
  - Intra-team communications—1 per individual (secure or nonsecure).
  - Cellular telephone.
- CI team to source—2 sets × CI team:
  - Phone cards.
  - Cell phones.
  - Radios.
  - Email or "Blackberry-like" communications.
  - One-way pager.

This page intentionally left blank.

Appendix I

Counterintelligence Special Agent Application Information Packet

This appendix provides information concerning how Soldiers can apply to become a military occupational specialty (MOS) 35L, counterintelligence (CI) special agent:

- Figure I-1. Information sheet—CI (MOS 35L).
- Figure I-2. Applicant information sheet.
- Figure I-3. CI special agent application—minimum qualifications.
- Figure I-4. CI applicant processing checklist.
- Figure I-5. CI special agent applicant—interview process.
- Figure I-6. Orientation statement.
- Figure I-7. Instructions for the contingency statement and compositions.
- Figure I-8. Final interview.
- Figure I-9. Final interview guide.
- Figure I-10. CI applicant interview biographic sheet.
- Figure I-11. Interview agent's post-interview requirements.
- Figure I-12. Statement of interview.
- Figure I-13. CI applicant HRC memorandum.

INFORMATION SHEET
COUNTERINTELLIGENCE (MOS 35L)

1. Purpose: The purpose of this appendix is to give Soldiers an overview of the MOS 35L including the prerequisites, MOS description, training, assignments, application procedures, acceptance for reclassification, retention in the MOS, and points to consider before making application.

2. MOS Description and type training:

a. Counterintelligence (CI) special agent (MOS 35L): CI is an activity that denies the enemy information about our plans, objectives, and strengths. It aims at defeating attempts against the United States by foreign nations and entities in the fields of espionage, foreign terrorists, sabotage, and subversion. The two phases of CI can be identified as: (1) the defensive measures taken to prevent information from falling into the hands of the enemy; (2) the active, or aggressive measures taken to eliminate, neutralize, or exploit enemy personnel or activities directed toward obtaining such information.

b. The CI special agent's training course includes training on countersabotage, counterterrorism, counterespionage, surveillance techniques, study of foreign intelligence services, US Army and foreign map reading, interview and interrogation techniques, legal principles, Army writing style, and a multitude of other related subjects. The course is approximately 18 weeks in duration and is conducted at the US Army Intelligence Center and School located at Fort Huachuca, Arizona. Upon acceptance by the Department of the Army (DA) for training, in-service transferees are issued temporary duty (TDY) assignment orders assigning them to Fort Huachuca enroute to their new permanent change of station (PCS). See DA Pamphlet 351-4, paragraph 3-12, US Army Intelligence Center and School (USAICS), Fort Huachuca, AZ 85613.

c. Types of assignments: MOS 35L personnel are assigned to all ASCCs, for example, US Army Forces Command elements, US Army Southern Command elements, US Army Pacific Command elements, US Army Europe elements, US Army Intelligence and Security Command elements to include tactical military intelligence (MI) organizations at Corps and below. Assignments are controlled by the Military Intelligence Branch, Enlisted Personnel Directorate, Human Resources Command. Assignments can include strategic as well as tactical assignments varying throughout the Army. **This MOS is one of very few in which your Daily Mission is your War Time Mission. You are constantly training to enhance your technical skills and ensure the safety of National Security.**

d. Duties:

(1) MOS 35L20: Conducts CI investigations.
(2) MOS 35L30: Conducts CI investigations.
(3) MOS 35L40: Supervises and conducts CI operations.
(4) MOS 35L50: Supervises CI operations.

3. Acceptance: Acceptance is contingent upon the following:

a. Applicants MUST fulfill the minimal requirements as listed on the "CI Agent Application Minimum Qualification" check sheet.

Figure I-1. Information sheet—CI (MOS 35L)

b. All documents as listed on the "CI Agent Application Required Documents Checklist" must be completed and turned into the CI special agent before conducting the interview.

c. Applicants must complete the Interview portion of the application process. The CI special agent will then complete the Statement of Interview and transmittal letter and send the applicant's packet to the MOS 35L Branch Manager.

d. The DA Branch Manager is the adjudicator and will review the applicant's packet and decide whether or not to accept the applicant. If accepted:

(1) The 35L Branch Manager will issue out an Advanced Individual Training (AIT) date to the applicant.

(2) The 35L Branch Manager will send the applicant TDY orders for attendance at the 35L, CI special agents Course (CISAC) AIT, Fort Huachuca, AZ.

4. Retention: The retention of a 35L is contingent upon the following:

a. A continuous military and criminal record free from indiscretion or defects of character that are deemed unacceptable for personnel engaged in duties prescribed by the MOS.

b. Continuation of eligibility for intelligence duties in accordance with prerequisites of the career group.

c. Satisfactory performance of duties and demonstrated career potential.

d. Continuation of eligibility with regards to spouse.

(1) Request for waivers will be submitted before marriage and will include an appropriate recommendation by the immediate commander. Waivers will be granted only when the overall value of the individual fully justifies his retention in the MOS. The value of his intelligence knowledge or skills as they relate to intelligence requirements will be considered in making the determination.

(2) After acceptance into MOS 35L, an individual who marries a foreign national or naturalized citizen who has not resided at least 5 years in the United States will become ineligible for duty unless granted a waiver by MILPERCEN. Pending approval of such requests by HQDA, the individual will be removed from sensitive duties.

e. Probation period: All newly accredited personnel will begin a one-year probationary period upon arrival at first operational duty assignment in a 35L position. During the probationary period, personnel will not be utilized on sensitive investigations except as required by special circumstances. A continual evaluation will be made of each individual's demonstrated overall performance, capabilities, and potential during this period. A specific, written recommendation will be submitted by each individual's commanding officer at the completion of the period stating whether or not the individual should be retained in MOS 35L.

f. Commanders of major commands may relieve personnel performing duties in a MOS listed in the 97-series and assign them to other duties for the following reasons:

(1) Expressed desire by the individual not to perform duties in his assigned MOS. This expressed desire is not to be used solely for the purpose of evading an assignment deemed unsatisfactory by the individual.

Figure I-1. Information sheet—CI (MOS 35L) (continued)

(2) Acts of disaffection, disloyalty or subversion.

(3) Character deficiencies, including indiscretions or propriety below the standards prescribed in this section.

(4) Undesirable mental attitude expressive of subversion, disloyalty, or disaffection.

(5) Loss of badge or credentials through negligence.

(6) Abuse of operational privileges granted to certain intelligence personnel.

(7) Demonstrated inability to perform duties commensurate with military grade and standards.

5. Considerations: Points you should take under careful consideration before making an application for MOS 35L:

a. If your motivation is strictly to get away from the normal Army routine, MOS 35L is not the career you are seeking. This MOS is not a "James Bond/Super Spook" type of MOS. MOS 35L personnel are service members of the Army. CI special agents are required to maintain the same standards in accordance with Army regulations as the remainder of the Army (for example, haircuts, uniforms). No subordinate branch performs our non-investigative duties, such as charge-of-quarters, maintenance of vehicles and equipment, and administrative issues. These tasks are the responsibility of the individual to complete. Approximately 40 percent of our assignments require the wearing of civilian clothing; however, an E-4 is still an E-4, an E-6 is still an E-6, and so on, and are assigned duties, responsibilities, accordingly.

b. Do you like to write and enjoy talking? Do you believe your interpersonal skills are exceptional? Do you have a problem with Professional Criticism? No investigation or operation begins before a plan submitted in writing. Approximately 60 percent of a normal duty day is used in writing reports. All information obtained through an interview, liaison, or observation must be recorded into written form. The possibility is always present of any report you produce becoming evidence in the court of law. Your report may also be the deciding factor in determining an individual's suitability or loyalty to the United States. The protection of classified information and/or material may depend on YOUR ability to gather the actual facts and express these facts in writing.

c. Some assignments place personnel, regardless of grade, in charge of a small office; for example, one- to four-person offices, to include all investigations. The responsibility is yours. No squad leader, platoon sergeant, first sergeant, or other is present for guidance. It will be your responsibility to ensure the job is completed in a timely fashion and meets all suspense dates.

d. Military Intelligence organizations establish the normal 8-hour duty day. However, due to our mission, this is not always the case. Following are a few examples:

(1) Some organizations require you to be within telephone contact at all times. If you leave your quarters during non-normal duty hours you may only go where you can be reached by telephone and you are required to report in each time you go from point to point.

(2) There are times when you will be required to remain at your place of duty until it is reasonable for you to either be relieved or the mission for the day is done. In certain situations, you will be eating dinner at the office. You stay until the mission is complete.

Figure I-1. Information sheet—CI (MOS 35L) (continued)

(3) In numerous military intelligence organizations it appears Saturdays and Sundays are the best days to catch up on backlog.

(4) Some assignments require frequent TDY trips, while some assignments, although non-TDY, may begin 100 miles from your office which means an added 3 or 4 hours to your normal duty day.

e. If you are married, it is recommended you discuss with your spouse the possible extended duty hours, irregular duty hours, and the possibility of frequent TDY trips. We like to maintain a happy "MI Family" and consider spouses a part of that family.

Note. This paper was not prepared to encourage or discourage your decision, but only to explain the facts as they exist.

6. References:

AR 600-200, *Army Command Policy*, June 2008.
AR 601-210, *Active and Reserve Component Enlistment Program*, June 2007.
AR 601-280, *Army Retention Program*, January 2008.
AR 611-1, *MOS Structure, Development & Implementation*, September 1997.
AR 614-200, *Chapter 6, Section I, Intelligence Career Program*, June 2007.
DA Pamphlet 351-4, Paragraph 3-12, USAICS&FH (Code: 301), pages 3-76 and 3-79, October 1995.
DA Pamphlet 600-8, Procedure 3-33, *Personnel Selection and Classification Interview Guide for Military Intelligence Applicants*, pages 3-221 through 3-245, August 1986.
DA PAM 611-21, *Military Occupational Classification and Structure*, January 2007.

7. Eleven-Step Process: Eleven Steps to transfer to MOS 35L. (All steps must be completed before contacting the Field Office). Reference: 1 August 1986 Update to DA Pam 600-8, 3-52 Procedure 3-31-1 AD.

a. Step 1:

Action Required by: Individual.
Description of actions: Inform immediate supervisor and Unit Commander of intention to volunteer for MI service. Currently not required, but recommended is for the future MI Applicant to take the Defense Language Aptitude Test at the Education Center.

b. Step 2:

Action Required by: Unit Cdr/1SG/BnPAC/PSNCO.
Description of actions: Assist Soldier in preparing DA Form 4187 requesting MI training. Privacy Act Statement will be furnished to Soldier before having individual complete DA Form 4187. (Done by your Personnel Administration Center [PAC]).

c. Step 3:

Action Required by: PSNCO.
Description of actions: Arrange an appointment with the S-2/G-2 or security manager for completion of SF 86 (EQSQ). Arrange an appointment with the photographic facility. The photograph is to be full length in Class "A" uniform (or their equivalent). No civilian clothing photograph is required.

Figure I-1. Information sheet—CI (MOS 35L) (continued)

d. Step 4:
Action required by: S-2/G-2/Security Manager.
Description of actions: Advise all applicants they must undergo a SSBI. Current information on security forms and number of required copies to initiate the investigations are contained in AR 604-5. Two completed copies of SF 86 (Questionnaire for National Security Positions). One copy will be original front and back.

Complete two copies of FD-258 (FBI Fingerprint Card). Ensure all personal history and physical characteristics blocks are completed and both individual and person taking fingerprints sign the appropriate signature blocks.

e. Step 5:
Action required by: Photographic Facility.
Description of actions: Prepare 3/4 length photograph of individual in Class "A" uniform (or their equivalent).

f. Step 6:
Action required by: PSNCO.
Description of actions: Upon completion of steps 4 and 5, arrange an appointment with MILPO. Have Soldier hand carry DA form 4187 with supporting documents to the MILPO.

g. Step 7:
Action required by: Personnel Management Specialist.
Description of actions: Obtain a MPRJ from Records Branch; Verify that Soldier meets eligibility criteria and prerequisites contained in section II, chapter 7, AR 614-200, DA Pamphlet 351-4, and the MOS requirements in AR 611-201; Ensure that SF 86, FD-258, and photograph are attached; Prepare forwarding comment to local supporting MI office. Reproduce and attach 1 copy of the Soldier's DA Forms 2 and 2-1 or ERB to the request.

h. Step 8:
Action required by: Personnel Management Supervisor.
Description of actions: Review documents to ensure tasks are completed.

i. Step 9:
Action required by: Personnel Management Officer.
Description of actions: Review and sign documents.

j. Step 10:
Action required by: Records Specialist.
Description of actions: File copy of request for MI training as action pending document in MPRJ.

k. Step 11:
Action required by: Personnel Management Specialist.
Description of actions: Arrange for an interview by an experienced CI Special Agent. On day of interview, have Soldier obtain MPRJ for review by CI Special Agent. Have Soldier take DA Form 4187 with enclosures to interview.

Figure I-1. Information sheet—CI (MOS 35L) (continued)

CI SPECIAL AGENT APPLICATION
INFORMATION SHEET

FULL NAME: _____

RANK: _____ **SSN:** _____
(Will sign Privacy Act Advisement; Privacy Act of 1974 applies)

UNIT ADDRESS: _____

UNIT PHONE #: _____ **UNIT Fax#:** _____

HOME ADDRESS: _____

HOME PHONE #: _____

AKO Email Address: _____

PMOS: _____

OTHER MOSs HELD: _____

DUTY POSITION: _____

ETS DATE: _____

DATE OF BIRTH: _____

PLACE OF BIRTH: _____

DRIVER LICENSE #: _____ **STATE:** _____

COMMANDER NAME, RANK, AND PHONE: _____

How did you hear about Counterintelligence/35L?

_____

_____

_____

_____

_____

Figure I-2. Applicant information sheet

Privacy Act Advisement

The authority for requesting the information during this interview is contained in Title 10, USC § 3012, and Executive Orders 9397, 10450, and 12065. The requested information will be used for making personnel security determination for membership in the Armed Forces of the United States and/or access to classified information, and for making personnel management decisions. The routine uses are for the determination of the scope and coverage of a personnel security investigation, assuring the completeness of investigations, and providing evaluators and adjudicators with basic personal history information relevant to security and suitability determinations. The information may be disclosed to other Federal agencies that are also charged with making the foregoing determinations.

Completion of this interview is voluntary. However, failure on your part to furnish all or part of the information requested may result in reassignment to non-sensitive duties or denial of access to classified information. At your request, a copy of this Privacy Act Advisement will be provided to you for your retention.

Signature of Applicant_____

Date_____

Figure I-2. Applicant information sheet (continued)

CI SPECIAL AGENT APPLICATION
MINIMUM QUALIFICATIONS

1. References: **AR 611-21**, **10-275b**

a. _____A physical demands rating of **Medium**.

b. _____A physical profile of **222221.**

c. _____Normal color vision.

d. _____A minimum score of **102** in aptitude area **ST/Technical** on the ASVAB.

e. _____A security clearance of **INTERIM TS** with eligibility for access to SCI once TS Clearance is granted.

f. _____A high school graduate or equivalent.

g. _____Possess good voice quality and be able to speak English without an objectionable accent or impediment.

h. _____Never been a member of the US Peace Corps.

i. _____No information in Provost Marshal, Intelligence, Military Personal Records Jacket, or medical records which would prevent the granting security clearance under **in accordance with AR 380-67**.

j. _____No records of conviction by court-martial.

k. _____No records of conviction by civil court for any offense other than minor traffic violations.

l. _____A US citizen by birth.

(1) *Members of immediate family (spouse, parents, brothers, sisters and children) must also be US citizens. Soldier and immediate family members can be naturalized citizens. If naturalized, there is no minimum residency requirement.*

(2) Soldier and spouse must not have immediate family members who reside in a country within whose boundaries where physical or mental coercion is known to be a common practice, ***either against:***

1. Person accused of or acting in the interested of the US.

2. The relatives of such persons to whom they may reasonably be considered to be bound by ties of affection, kinship, or obligation. Near relatives will also include uncles, aunts, grandparents, father-in-law, mother-in-law, and relationships corresponding to any of the above persons in loco parentis (AR 630-5 and 37 USC 501).

Figure I-3. CI special agent application—minimum qualifications

m. _____ Have neither commercial nor vested interest in a country within whose boundaries physical or mental coercion is known to be a common practice against persons acting in the interest of the US This requirement applies to the Soldier's spouses as well.

n. _____ A minimum age of 21 years of age for award of MOS 35L accreditation as a CI Special Agent.

o. _____ **Have an ACTIVE Army Knowledge Online (AKO) email account. If you do not have an AKO email account when you packet is sent forward, you packet will** not be processed.

p. ____ To qualify under the BEAR program (if applicable) the Soldier must have less than 10 years of service at time of reenlistment on the day of graduation from school.

2. Any question concerning these minimum requirements please contact your local CI office.

Figure I-3. CI special agent application—minimum qualifications (continued)

CI Applicant Processing Checklist

1. Orient the application on the general CI mission and the duties and functions of CI Special Agents.
2. Answer all the applicant's questions on career opportunities within classification limitations.
3. During the processing, afford the applicant the opportunity to withdraw his application.
4. Inform the applicant to contact you if, at any time, he decides not to accept his obligation to serve in Military Intelligence.
5. Review the application packet for applicant eligibility and background information.
6. Advise the applicant of any waivers required.
7. Advise the requesting agency of applicant ineligibility for and requirements that cannot be waivered.
8. Advise the applicant of the SSBI requirement; the minimum age requirement of 21; the continuing assessment of applicant during his training; the one-year agent probationary period; and the continued retention requirements.
9. Give the applicant a Privacy Act Advisement before the solicitation of any personal information.
10. Obtain a signed Contingency Statement from the applicant.
11. Conduct the interview.
12. Ensure the preparation of the Soldier's composition within a controlled environment and review them.
13. Make no promises concerning applicant's acceptance or future assignments.
14. Prepare the Statement of Interview.
15. Determine for yourself before recommending the applicant for CI Special Agent duties that he possesses all the traits, skills, and characteristics desired of a CI Special Agent.
16. Forward the Statement of Interview and a letter of transmittal via Federal Express to:

ACTIVE DUTY:
Commander, HRC-Alexandria
ATTN: AHRC-EPB-M Z (35L)
2461 Eisenhower Avenue
Alexandria, VA 22331-0400
Comm: 703.325.4983

Figure I-4. CI applicant processing checklist

RESERVE/NATIONAL GUARD:
U.S. Army Human Resources Command—St. Louis
ATTN: AHRC-PLF
1 Reserve Way
St. Louis, MO 63132-5200
Comm: 314.592.0255

17. Ensure copies have been retained to keep on file at FKFO for 1 year.
18. Inform the applicant, his/her commander, and his/her retention NCO that his/her packet has been forwarded to the MI Branch Manager.

Figure I-4. CI applicant processing checklist (continued)

INITIAL INTERVIEW

1. The Initial Interview is the first interview to explain to the prospective CI applicant about the mission of Army CI, the requirements for becoming a CI Special Agent, and the process that must be completed to be accepted into the Army CI Program, training, and potential assignments. CI Special Agents processing CI applicants will ensure they do not form any positive or negatives biases towards a potential CI applicant. They should be afforded the opportunity to apply for the CI Program. Failure to meet requirements or lack of character traits that would preclude from being a professional and competent CI Special Agent will be developed during the course of the CI applicant process. Because CI is not an initial entry MOS, the CI applicant process is important in maintaining the CI MOS and more importantly maintaining the CI MOS with the most qualified and competent personnel in the Army's ranks.

- Answer all of the potential applicant's questions pertaining to the field. Orient the Soldier on the general mission and functions of the US Army CI, to include the duties and functions of a CI Special Agent (35L10-35L50). Advise the applicant of both the tactical and strategic missions of a CI Special Agent.
- Make no promises concerning potential applicant's acceptance or future assignments.
- Direct potential applicant to the G-2/S-2/Post Security Office for Security Clearance application. Inform applicant that upon completion of Security Clearance packet he/she should obtain a complete copy from the G-2/S-2/Post Security Office and bring it with him/her for the next interview.
- Provide the potential applicant with current application required documents and minimum qualification checklist. Be sure to inform the applicant that one complete copy must be provided to the interviewing agent and will not be returned, regardless of the adjudication.

Figure I-5. CI special agent applicant interview process

PROCESSING INTERVIEW

2. The Processing Interview is conducted after the CI applicant has completed all the administrative tasks outlined in the CI Applicant Information Packet. Generally on those personnel who are serious about applying for and being accepted into the CI Program will make it to this interview. During the processing interview:

- Afford the applicant the opportunity to withdraw his application.
- Applicant should have the following documents:
  - DA photo.
  - Enlisted record brief.
  - DA Form 4187 (Personnel Action).
  - SF 86 (Electronic Personnel Security Questionnaire).
  - FD-258 (FBI Fingerprint Card).
  - Copy of the interim TS clearance.
  - DLAB test results (optional).
- Review the application packet for applicant eligibility and background information.
- Check packet for all required documents.
- Check that documents are completed and filled out properly.
- Have applicant read and sign the Privacy Advisement before the interview.
- Have the applicant read and sign the Orientation Statement.
- Have applicant write up a Contingency Statement in his own handwriting and have him sign it and date, completed in pen). Contingency Statement found in DA PAM 600-8.
- Have applicant write a Motivational Composition (10-minute time limit), completed in pencil. Composition should state why he is applying for the position of a CI Special Agent.
- Biographical Composition (45-minutes time limit), completed in pencil. Composition should cover in as many paragraphs as necessary the following:
  - Family background and other influences during applicant's maturation.
  - The level of formal education attained.
  - Major fields of study.
  - Overall academic standing in high school and college.
  - How the education was financed.

Note 1. In which course(s) did applicant receive his best and worst grades and the reasons therefor.
Note 2. If formal education has not been completed, the reasons for leaving and intentions regarding completion.

3. Major career and employment fields in which applicant has been employed, to include—

- A brief description of duties performed.
- Length of time engaged in each field.
- Whether part-time, full-time, summer employment, or salary.
- Highest degree of responsibility assumed.
- Reasons for termination of employment.

Note 3. Inform the applicant to contact you if, at any time, he decides not to accept his/her obligation to serve in the Military Intelligence.

Figure I-5. CI special agent applicant interview process (continued)

ORIENTATION STATEMENT

1. I acknowledge that the following requirements for assignment to and retention for SCI duties have been explained to me:

a. If my application is approved for controlled intelligence MOS duties, I understand that I may be required to enlist, reenlist, or adjust my period of service as required under appropriate Army regulations.

b. I understand that I must meet the minimum established academic standards for the course of instruction for which I am selected to be retained in MI duties. Further, I understand that if I fail to complete the course of instruction for any reason, I will be required to complete my term of service. I understand that after I satisfactorily complete the school training, I will be assigned in accordance with the needs of the Army. I acknowledge that no promises have been made to me as to area of assignment nor the exact type of duties to be performed.

c. I also understand that Joint Travel Regulations prohibit the transportation of my spouse and family members and shipment of household goods at government expense to school courses of less than 20 weeks duration.

d. I understand that MI personnel who marry (by religious or civil ceremony or under the common law) any person not a United States citizen by birth or a naturalized citizen will become ineligible automatically for continued duty in controlled intelligence MOS unless granted a waiver by the Commanding General, US Total Army Personnel Command.

2. I have been informed and understand that actual assignment to, and retention in, controlled intelligence duties of any individual, including enlistees for such training and duties, will depend on the following:

a. Favorable results of special background investigation (SBI) initiated and controlled by the Chief, Military Intelligence, US Army, to include an evaluation of my personal characteristics and potential capabilities.

b. Successful completion of prescribed course of instruction.

c. Good moral character.

d. Integrity of a degree commensurate with the recognized high standards for intelligence duties as required by the nature of intelligence operations.

e. Satisfactory performance of assigned intelligence duties.

f. Continuance of eligibility for assignment in accordance with prerequisites listed in AR 614-200 or AR 614-103.

Figure I-6. Orientation statement

g. All newly accredited personnel begin a one-year probationary period beginning the first day of duty following award of PMOS, or until 21 years of age, whichever is longer.

3. I have been further advised and understand that:

a. Failure to meet and adhere to any of the above requirements will result in my reassignment from controlled intelligence MOS duties. If reassignment is necessary, I will not be given further choice of assignment, but will be reclassified and reassigned in accordance with the needs of the Army and required to complete the term of service.

b. Final determination or retention for MI duties will be made by the Commanding General, US Total Army Personnel Command. Enlistment and subsequent assignment to Fort Huachuca, AZ, in itself should not be construed as assurance of acceptance for intelligence MOS duties.

4. I have been informed that the intelligence course is taught at the US Army Intelligence Center and School, Fort Huachuca, AZ.

5. I have read and understand the above information.

_____	_____
Signature of Applicant	Signature of Witness (Interviewer)
_____	_____
Printed Name of Applicant	Unit
_____	_____
Applicant's Address	Date

Figure I-6. Orientation statement (continued)

INSTRUCTIONS FOR THE CONTINGENCY STATEMENT AND COMPOSITIONS

1. As part of your processing for Military Intelligence duties you are required to complete a Contingency Statement in your own handwriting and to write two compositions within prescribed time limits. You have been supplied the following materials to complete the required statement and compositions:

- A black ballpoint pen.
- Bond paper.
- Sharpened pencil.

2. **Contingency Statement:** As part of your processing, the following **Contingency Statement must be completed in ink** on a separate sheet of paper in your own handwriting and signed and dated.

Contingency Statement
…(Date)…

"I understand that final acceptance for duties as a CI Special Agent is contingent upon a favorable special background investigation (SBI), including an evaluation of my personal characteristics and potential capabilities, and successful completion of a prescribed course of instruction. I also understand that the type of training within the CI Special Agent field I receive is at the discretion of the Department of the Army."

…(Signature of applicant)…

********COMPLETE THE CONTINGENCY STATEMENT IN PEN AT THIS TIME*******

3. **Compositions:** The purpose of the two compositions is to determine how well you are capable of reasoning and expressing yourself in writing and to determine your use of English grammar and punctuation. Content, construction, clarity, conciseness, completeness, spelling, and maturity of thought expression are principal areas of interest.

a. **General Instructions:**

(1) Write your last name and date at the top right hand corner of each sheet of paper that is used for your compositions. Number each page at the bottom.

(2) As you finish each composition, sign your name and print your full name and service number.

(3) You will be timed by the interviewer.

b. **Motivational Composition *(10-minute time limit):***

Write a one paragraph composition stating why you are applying for CI Special Agent duties.

**************COMPLETE THE COMPOSITION IN PENCIL AT THIS TIME***************

Figure I-7. Instructions for the contingency statement and compositions

c. **Biographical Composition** ***(45-minute time limit):***

Write a biographical composition in as many paragraphs as necessary to cover the following facets of your life:

(1) Describe your family background and other influences during your maturation.
(a) The level of formal education attained.
(b) Major fields of study.
(c) Overall academic standing in high school and college.
(d) How the education was financed.
(e) In which course did you receive your best and worst grades and the reasons therefor?
(f) If formal education has not yet been completed, the reasons for leaving and intentions regarding completion.

(2) Major fields in which you have been employed (for example, sales, office work, farming, laborer) to include—
(a) A brief description of duties performed.
(b) Length of time engaged in each field.
(c) Whether part-time, full-time, or summer employment.
(d) Highest degree of responsibility assumed.
(e) Reasons for termination of employment.

(3) Describe the major incidents in your life which have affected your personality, character, or your outlook on life.

(4) Describe your major interests in life and what has been done to develop them.

**********COMPLETE THE COMPOSITION IN PENCIL AT THIS TIME**********

Figure I-7. Instructions for the contingency statement and compositions (continued)

FINAL INTERVIEW

The Final Interview is the final coordination between the interviewing CI Special Agent and the CI applicant. The Final Interview is conducted when all documentation has been completed by the CI applicant and the interviewing agent has had the opportunity to review and assemble the packet to forward to Human Resources Command (HRC) for final approval and/or disapproval. While the interviewing agent may have already written his/her recommendation on approval or disapproval, this should not be provided to the CI applicant.

1. Afford the applicant the opportunity to withdraw his application.

2. Have applicant read and sign the Privacy Advisement before the interview, if not done so in the Processing Interview.

- Before this interview—
- Ask applicant for any and all information not given before that would be pertinent to his/her application packet (things that could disqualify applicant).
- Inform him/her that upon completion of the Packet you will inform him/her as to the disposition of their packet and when it was forwarded to HRC.
- Send Transmittal Letter to the applicant's commander and retention NCO.

3. Inform the applicant to contact you if, at any time, he decides not to accept his/her obligation to serve in the Military Intelligence.

Figure I-8. Final interview

FINAL INTERVIEW GUIDE

1. Interview:

a. Upon being interviewed for MOS 35L, the interviewer will conduct the interview so it provides an opportunity to—

(1) Closely observe and evaluate the applicant.
(2) Elicit certain information that can be obtained through informal discussion with the applicant.

b. Exploit the following areas fully:

(1) Family background of applicant.
(2) Personal problems which limit the usefulness of applicant in intelligence duties.
(3) Linguistic ability and how acquired.
(4) Financial responsibility.
(5) Association with the opposite sex.
(6) Participation in sports.
(7) Courses of study, technical training, or other skills or hobbies which enhance the applicant's potential for intelligence duties.
(8) Knowledge and interest in political and world affairs.
(9) Reserve Officers Training Corps (ROTC) experience to include responsible positions held and reasons for leaving.
(10) Applicant's reason and basic motivation for applying for intelligence duties and the training he desires (specific course).
(11) Whether he possesses a valid driver's license.
(12) Motivation and reasons for applying for MOS 35L, poise, mental alertness, sincerity, ability to think quickly, ability of oral expression, personality, and maturity.

c. The qualities and attitudes listed below are desirable and particularly sought by Military Intelligence:

(1) **Neatness** (clean-shaven, shoes polished, brass polished, clothing clean and pressed, hair combed, and neat, and clean hands and fingernails).
(2) **Posture** (erect, shoulders, back).
(3) **Stature and physique** (as outlined in AR 40-501 with special exception as to minimum requirements).
(4) **Physiognomy** (unscarred, unmarked, no outstanding characteristics to the extent the individual could be readily identified or cause him to stand out in a crowd).
(5) **Demeanor** (straightforward, looks directly at the interviewer when speaking, calm, poised, at ease, self-confident, courteous, respectful, pleasing (not servile), animated, interested, voice quality (well modulated), no unpleasant qualities or unusual characteristics which cause easy identification or undue qualities or unusual characteristics which cause easy identification or undue notice to the extent that it would be detrimental to the applicant's military intelligence duties).

Figure I-9. Final interview guide

d. Education:

(1) Attended accredited schools or received proper tutoring of self-instruction comparable to formal education requirements.
(2) Received passing grades in most subjects, especially English, History, and Political Science courses.
(3) Worked toward a definite goal.
(4) Intends to use his education to further his career.
(5) Expresses intention of completing or improving his education.
(6) Has retained a fair amount of what he learned in school.
(7) Has ability to write correctly, using good grammar and spelling.
(8) Speaks English correctly.

e. Development:

(1) Current events (well informed on current events, interested in national affairs, possess ability to reason and form conclusions relative to world affairs).
(2) Personal (has common sense, is quick to grasp a situation and quick to change his thoughts to new trends or changes in situations under discussion).

f. Composition: During the interview the applicant will be required to write two compositions: One consisting of one paragraph "Why I am applying for MOS 35L." The second composition will be written concerning the applicant's education, employment, and biographical background. The purpose of the composition is to determine how well the applicant expresses himself and his use of the English grammar and punctuation. Content, construction, clarity, conciseness, completeness, spelling, and maturity in thought expression are graded areas. (A Time limitation for the first composition is 10 minutes and for the second composition is 45 minutes.)

(1) Educational areas which will be included are—

- The level of formal education attained.
- Major fields of study.
- Overall academic standing in high school and college.
- How education was financed.
- Courses in which best and worst grades received and reasons therefor.
- If formal education has not been completed, reasons for leaving and intentions regarding completion.

(2) Major fields in which applicant has been employed (for example, sales, office work, farming, laborer, other) to include—

- A brief description of duties performed.
- Length of time engaged in each field.
- Whether part-time, full-time, or summer employment.
- Highest degree of responsibility assumed.

Figure I-9. Final interview guide (continued)

g. The applicant will also be required to complete a “Contingency Statement” and sign an “Orientation Statement” as part of the interview.

h. Upon completion of the applicant’s interview, the interviewer will prepare a “Statement of Interview” which includes the interviewer’s recommendations. The applicant’s CI packet will then be forwarded through MI channels, directly to PERSCOM. If recommended, a copy of the cover sheet will be given to the applicant’s commander and his/her retention officer.

Figure I-9. Final interview guide (continued)

CI APPLICANT INTERVIEW BIOGRAPHIC SHEET

PART 1—PERSONAL INFORMATION

FULL NAME: _____

RANK: _____ **SSN:** _____
(Will sign Privacy Act Advisement)

UNIT ADDRESS: _____

RESIDENCE: _____

PART 2—SOI DATA

DOB: _____ **POB:** _____

CITIZENSHIP: _____

HEIGHT: _____ **WEIGHT:**_____ **BUILD:**_____

COLOR VISION: _____

IDENTIFYING MARKS (Tattoos, Scars): _____

GT SCORE: _____ **ST SCORE:** _____

BASD: _____ **DLAB (Date and Score):**_____

LANGUAGE: _____

PMOS: _____ **SMOS:**_____

ETS: _____
DEROS:_____

DRIVERS LICENSE (and State):_____

PEACE CORP ASSOCIATION: _____

HIGHEST LEVEL EDUCATION ACHIEVED: _____

Figure I-10. CI applicant interview biographic sheet

PART 3—FAMILY BACKGROUND: (Name, POB, Residence, Occupation)

SPOUSE: _____

CHILDREN:

_____

_____

_____

FATHER:

_____

MOTHER: _____

BROTHERS/SISTERS:

_____

_____

_____

_____

SPOUSE'S FATHER: _____

SPOUSE'S MOTHER: _____

SPOUSE'S BROTHERS/SISTERS:

_____

_____

_____

_____

PART 4—FOREIGN

Do you or members of your family have commercial or vested interests in any foreign country?

Do you or members of your family have any relatives or friends residing outside the United States or that are not United States citizens?

Have you or your family traveled outside of the United States?

Figure I-10. CI applicant interview biographic sheet (continued)

PART 5—EDUCATION: (Include All Schools Attended)

ELEMENTARY SCHOOL(S): Dates, Names, Locations

_____
_____
_____
_____
_____
_____

HIGH SCHOOL(S): Dates, Names, Locations

_____
_____
_____
_____
_____
_____

COLLEGE(S): Dates, Names, Locations

_____
_____
_____
_____
_____
_____

GRADES: **HIGH SCHOOL** **COLLEGE** **OTHER**

ENGLISH_____

MATH_____

HISTORY_____

POLSCI_____

OTHER_____

TECHNICAL OR CORRESPONDENCE COURSES: Dates, Names, Locations

_____
_____
_____
_____
_____
_____

Figure I-10. CI applicant interview biographic sheet (continued)

What class or subjects were you most interested in and why?

What class or subjects were you the least interested in and why?

What class or subjects did you excel in and why?

What class did you do the poorest in and why?

What goals were you working toward in High School, College, etc.?

Did you take any languages in school?

Do you intend to complete or improve upon your education and how?

How do you intend to use your education to further your career in the Army and civilian world?

***Has the applicant retained a fair amount of what he/she had learned in school?**

***Does the applicant have the ability to write correctly using good grammar and spelling?**

What courses of study, technical training or other skills do you have that would enhance your potential for intelligence duties?

Did you participate in any sports in school or in your community?

Do you have any ROTC experience?

Figure I-10. CI applicant interview biographic sheet (continued)

PART 6—EMPLOYMENT

What, where, when, part time or full time, reason for leaving, position held (as complete as possible):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

PART 7—FINANCIAL RESPONSIBILITY (see attached financial sheet)

INCOME (include all):

MILITARY: _____

OTHER: _____

MONTHLY BILLS (Who, what, and how much):

_____
_____
_____
_____
_____

OTHER DEBTS (Who, what, and how much):

_____
_____
_____
_____

Figure I-10. CI applicant interview biographic sheet (continued)

FINANCIAL SHEET

NAME: _____

DATE OF INTERVIEW: _____

NAME OF CREDITOR:_____

ADDRESS: _____

ACCT#:_____

Date acct. Opened: _____
Initial Balance:_____
Highest Balance:_____
Current Balance:_____

Original repayment terms: _____
_____

Any charges in repayment terms: _____

Date of most recent payment: _____

Current account status: _____
_____

Cause of the financial problems (in detail):
_____
_____
_____

If you can pay: _____

Actions Already taken:
_____
_____
_____
_____

Figure I-10. CI applicant interview biographic sheet (continued)

Intentions to repay:

_____
_____
_____

PART 8—CLUBS, ORGANIZATIONS, ACTIVITIES

Are you currently, or have you ever been in any club, organization or group activity?

Have you ever been associated with any individuals who are known to be, or have reason to believe they could be, or have been, members of any organization which advocates the overthrow of our constitutional form of government? Explain.

_____
_____
_____

PART 9—CRIMES AND PUNISHMENT

Have you ever been detained, held, arrested, indicted, or summoned to court as a defendant in any criminal proceeding?

Have you ever been convicted, fined, or imprisoned or placed on probation or have been ordered to deposit bail or collateral for the violation of any law, police regulation or ordinance? Explain.

Have you ever been given an Article 15?

Have you ever been ordered to appear before, charged by, or convicted in a Military Court?

Have you ever been ordered to appear before, charged by, or convicted in a Civil Court?

Have you ever received any traffic violations? If so, what were they for and are any of them still pending?

Figure I-10. CI applicant interview biographic sheet (continued)

PART 10—LIFE EXPERIENCES

Are there any incidents in your life which may reflect adversely upon your loyalty, integrity, or discretion?

Do you have any personal problems which would limit your usefulness as an agent in Military Intelligence?

Have you ever used, sold, or trafficked any illegal drug, narcotic, or hallucinogen, to include marijuana or hashish? (Abuse of prescribed drugs, experimentation, etc.)

Do you drink alcoholic beverages? (Frequency, what kind, under what conditions?)

Do you have any political or religious views that would preclude you from carrying out assignments if accepted into Military Intelligence?

Have you ever gone to or been directed to see and talk with a psychologist or psychiatrist and why?

PART 11—MORALS

What are your views on racial matters?

Do you judge individuals on their own merit?

Do you have a problem working with a member of the opposite sex?

PART 12—KNOWLEDGE AND INTEREST IN POLITICS AND WORLD AFFAIRS

What do you consider to be an important current event in national affairs? Why?

What do you consider to be an important current event in international affairs? Why?

If you had the authority to change any US government policy or procedure, what would you change and why?

How do you gain your knowledge of politics and world affairs?

Figure I-10. CI applicant interview biographic sheet (continued)

PART 13—MILITARY

What is the NCO's obligation to his/her commander? To his/her troops?

In a combat situation, would you take up arms against the enemy?

PART 14—FINAL DISCLOSURE

Is there any information that you feel you need to disclose that would be or could be pertinent to you working in Military Intelligence?

PART 15—AGENT OBSERVATION

PERSONAL:

Ability to reason and form conclusions

Has common sense

Quick to grasp situation

Quick to change thought to new trends or changes in situation under discussion

Oral expression, ability to verbalize

Mental alertness

Personality

Maturity

Sincerity

Sense of Responsibility

Figure I-10. CI applicant interview biographic sheet (continued)

APPEARANCE:

Posture

Physiognomy

Neatness (clean shaven, clothing clean and pressed, hair combed and neat, etc.)

DEMEANOR:

Straightforward

Maintains eye contact

Calm

Poise

At ease

Self-confident

Courteous

Respectful

Voice quality

CURRENT EVENTS:

Well informed

Interest in national and international affairs

What is their reason for wanting to become a CI Agent? How did they become aware of MI?

WAIVERS:

RECOMMENDATION:

Figure I-10. CI applicant interview biographic sheet (continued)

INTERVIEWING AGENT'S POST-INTERVIEW REQUIREMENTS

1. Make copies of packet to be maintained on file, Keep for one Fiscal Year.

2. Type **Statement of Interview**.

3. Type **Letter of Transmittal** with approval or disapproval.

4. Forward the applicant's packet via (FedEx) to:

ACTIVE DUTY:
Commander, HRC-Alexandria
ATTN: AHRC-EPB-M (35L)
2461 Eisenhower Avenue
Alexandria, Virginia 22331-0400
Comm: 703.325.4983

OR

RESERVE/NATIONAL GUARD
US Army Human Resources Command – St. Louis
ATTN: AHRC-PLF
1 Reserve Way
St. Louis, MO 63132-5200
Comm: 314.592.0255

5. Forward a copy of the Letter of Transmittal to the applicant's Commander and inform the commander that we are not the adjudicators. Acceptance or Disapproval will be in form of a Memorandum for Record and/or phone call to the applicant's commander or notification through AKO.

6. File a complete copy of the MI applicant's packet under MARKS 611-201a and store for one fiscal year and then destroy. The Letter of Transmittal MARKS is 614-200a and is stored at the DA level.

7. **If an MI applicant decides to pull his/her Applicant Packet from consideration, email the current Branch Manager a short memorandum stating why. This is twice as important if the applicant was not going to be recommended. Keep a copy of the email in the MI Applicant's local file for 1 year.**

Figure I-11. Interviewing agent's post-interview requirements

*****Official Letterhead*****

REPLY TO
ATTENTION OF:

IAMG-B-FK (TNR-12) 11 June 2002

SUBJECT: Statement of Interview

1. On 11 June 2008, Joshua J. Doe; SGT; 123-45-6789; A Company, 2d Battalion, 187th Infantry, 101st Airborne Division, Bldg. 6920 Desert Storm Avenue, Fort Knox, KY 42223; an applicant for Career Management Field 96, MOS 35L, CI Agent, was interviewed.

2. The following information is submitted:

a. DOB: 09 April 1800
b. POB: North Conway, New Hampshire
c. Citizenship: US
d. Height: 68”
e. Weight: 170
f. Build: Medium
g. Physical Profile: 111111
h. Color Vision: Normal
i. ST Score: 121
j. BASD: 09 August 1997
k. DLAB: 118
l. Language: NONE
m. PMOS: 11B20
n. ETS: 1 December 2000
o. Peace Corps: No
p. Years Formal Education: 12
q. AKO email address:
r. Driver’s License Number/State:

3. The results of the interview with SGT Doe are as follows:

a. Background:

(1) SGT Doe was born on 4 April 1973 to the parents of Kerry Lee and John William Doe in North Conway, New Hampshire. Approximately two years later, SGT Doe’s family moved to Rhode Island. SGT Doe spent the majority of his life growing up in Rhode Island. SGT Doe comes from a very strong family background. SGT Doe spent a lot of time with his family taking vacations visiting, and skiing during their annual ski trip. His parents have been married for 28 years. SGT Doe, has one brother named Nicholas John Doe, and one sister named Jennifer Lee Doe. Mr. Doe believed in education and encouraged his children to always pursue their education and go to college. SGT Doe has a close relationship with his family and maintains weekly contact. The close relationship with his family has instilled in SGT Doe a high ethical and moral standard. SGT Doe considers his family to be his backbone,

Figure I-12. Statement of interview

IAMG-B-FK (TNR-12) 11 June 2002

SUBJECT: Statement of Interview

strength, and support network. His family supported his decision to join the Army.

(2) SGT Doe has transferred this strong sense of family over to his own family. SGT Doe married Treva Ann Doe (HER maiden name) on 25 January 1999. SGT Doe and his wife have a strong relationship and he does not feel that a deployment of any length would have an adverse effect on his marriage. SGT Doe has a stepchild named Richard Alan Sheets whom he loves as his own.

(3) SGT Doe does not have any foreign relatives or connections.

(4) SGT Doe does not have any personal or marital problems in his life that would prevent him from deploying anywhere in the world.

(5) SGT Doe does not have excess debt or any unpaid bills. He is financial responsible and pays his bills on time. SGT Doe has not had any bills referred to a collection agency.

b. Educational Background:

(1) Secondary, College, High School: SGT Doe attended Warwick Veterans Memorial High School in Rhode Island. His parents sent him to this school so he could compete on the school ski team. SGT Doe believes that attending the boarding school and competing on the ski team helped him to learn self-discipline and self-reliance. SGT Doe did well in the majority of his classes; however, he has always had a difficult time with mathematics. SGT Doe took college preparatory classes, but he did not have a desire to attend college. SGT Doe graduated High School on 25 June 1991. SGT Doe took a year off from school and entered the work force. On 15 September 1992, SGT Doe attended the Community College of Rhode Island. He attended the community college for three years. During that period, he completed most of his basic college courses. On 1 September 1995, SGT Doe transferred his college credits to Salve Regina University. He has completed 85 semester hours and is pursuing a BA with a concentration in law.

(2) Linguistic ability: SGT Doe does not speak any foreign languages at this time. He did score 118 on the DLAB.

(3) Subjects: SGT Doe did well in the majority of subjects in school. His only weakness appears to be mathematics. SGT Doe has a hard time working with equations and numbers. He can perform basic mathematical functions; however, he does have trouble with Algebra and calculus. SGT Doe has not demonstrated a deficiency with reading or writing the English language.

(4) Specific Courses: During High School and college, SGT Doe worked with the Law Enforcement Explorers. This organization takes high school and college students and encourages them to pursue a career in law enforcement. He participated in the ride-along program, attended meetings with law enforcement officials, and worked in a police

Figure I-12. Statement of interview (continued)

IAMG-B-FK (TNR-12) 11 June 2002

SUBJECT: Statement of Interview

department. After he reached the age of 21 he could no longer be a member of the organization so he worked as a counselor and mentor for the program.

(5) Future Plans: SGT Doe plans to stay in the Army pursuing a career in CI. He hopes to one day attend Warrant Officer Candidate School. He plans to finish his education and receive a BA with a law enforcement emphasis.

(6) Hobbies: SGT Doe enjoys skiing and playing sports and spending time with his son.

c. Employment Background:

(1) Full Time Employment:

(a) SGT Doe worked for Hotel Viking located in on 1 Bellevue Avenue, Newport, Rhode Island. His primary duty title was waiter. He had the responsibilities to take orders, serve food, and provide customer service.

(b) SGT Doe also worked for the Marriott Hotel, 24 Americas Cup Avenue, Newport, Rhode Island. His first duty position was engineer and there he worked around the hotel repairing items and keeping the grounds. As time progressed he was promoted to Security Officer and his primary responsibilities were providing security for the hotel and their guests. He also conducted investigations on employee theft.

d. Military Background: SGT Doe entered the Rhode Island National Guard on 7 March 1992. SGT Doe realized that he needed to further his education to get ahead in life so he joined the National Guard to get assistance for school. SGT Doe entered the guard as a 95B10 and he attained the rank of SPC/E-4. SGT Doe enjoyed being in the military and decided that he wanted to make the military a career so he applied for Active Duty. On 2 December 1997, SGT Doe entered Active Duty and was reassigned the MOS 11B. Since he was in the National Guard, the Army as that as prior service so he had to come on Active Duty according to the needs of the Army. The Army needed 11B so he became an 11B. His first duty station was B Company 1/506th Infantry Camp Greaves, Korea. He served in Korea from December 1997 to December 1998. After his tour in Korea, he was reassigned to 2/187th Infantry Fort Knox, KY. During his military career, he has received three Army Achievement Medals, one Overseas Ribbon, and the Army Service Ribbon.

e. Loyalty, Integrity, Discretion, Morals, and Character:

(1) Foreign Travels, business connection, and friends: SGT Doe has not traveled outside the United States outside of official military duties. He does not have any foreign business connections, contacts, friends, or families.

Figure I-12. Statement of interview (continued)

IAMG-B-FK (TNR-12) 11 June 2002

SUBJECT: Statement of Interview

(2) SGT Doe has been a member of Law Enforcement Explorers. This organization encourages youth to pursue careers in law enforcement. He is not a member of any organization that discriminates or advocates violence of any kind based on religion, race, sex, or beliefs.

(3) SGT Doe has not used any illegal substances, drugs, or intoxicants.

(4) SGT Doe is not involved in any gambling activities or actions that might make him susceptible for black mail.

(5) SGT Doe has never been charged or convicted of a felony offense nor has he been arrested. He has never been convicted of an offense involving alcohol or drugs.

(6) SGT Doe has never received psychological treatment.

(7) SGT Doe has not exhibited any actions nor been involved in any incidents, which would reflect unfavorably on his ability to perform as a CI agent.

f. Other Information:

(1) SGT Doe arrived 15 minutes early and had all of his paper work organized. He had a good shine on his boots and he had a pressed uniform.

(2) He had excellent military bearing and spoke extremely well. He answered the questions truthfully and without hesitation. He wants to retire from the Army as a CI Warrant Officer.

(3) He was articulate and expressed his views and beliefs in a professional manner.

(4) He has demonstrated average writing ability. However, he is an extremely hard worker and he continues to improve on his writing skills. He does not have a problem with spelling; he was a little weak on grammar.

(5) Current affairs: Not applicable.

(6) He is extremely adept at following changes in conversation, analyzing information, and developing sound solutions to problems.

(7) He is of extremely high moral character and this is demonstrated in his demeanor, appearance, and family history.

(8) He wants to pursue a career in the Army as a CI agent culminating in acceptance to Warrant Officer Candidate school.

Figure I-12. Statement of interview (continued)

IAMG-B-FK (TNR-12) 11 June 2002

SUBJECT: Statement of Interview

4. SGT Doe is looking for an exciting new change in his Army career. He has always had an interest in investigations and law enforcement. He has looked into the Criminal Investigation Division, but he was looking for a field that combined both intelligence and investigations.

5. Recommendation: I strongly recommend SGT Doe for assignment to CI duties. He is highly motivated, goal oriented, and is constantly seeking new challenges. He has a strong work ethic and is a constant professional.

YOUR NAME
RANK, Army
CI Special Agent

Figure I-12. Statement of interview (continued)

Official Letterhead

REPLY TO
ATTENTION OF:

IAMG-B-FK (614-200a) 11 June 2002

MEMORANDUM FOR COMMANDER, HRC – Alexandria, AHRC-EPB-M (35L) (SFC Moore), 2461 Eisenhower Avenue, Alexandria, VA 22331-0400

SUBJECT: Application for CI Special Agent

1. I have reviewed the attached application pertaining to John Q. Public, SPC, 123-45-6789, Company A, 2-327 Infantry Brigade, 101st Airborne Division (Air Assault), Fort Knox, KY 42223 and concur (non-concur) in the recommendation of the interviewer (or in the event of non-concurrence add reasons why).

2. (If SAIC does the interview) Forwarded herewith is the application pertaining to John Q. Public, SPC, 123-45-6789, Company B, 2-327 Infantry Brigade, 101st Airborne Division (Air Assault), Fort Knox, KY 42223.

3. Upon acceptance or non-acceptance the following unit commander is to be notified: CPT Stanley G. Jones, DSN 635-0000.

4. POC for this memorandum is the undersigned at DSN 624-3991.

13 Encl
1. Statement of Interview
2. Contingency Statement
3. Motivational Composition
4. Biographical Composition
5. Orientation Statement
6. Privacy Act Advisement
7. DA Form 4187
8. Standard Form 86
9. FD-258 FBI Fingerprint Cards
10. ERB
11. 2-1/2-A
12. Picture

CF minus Encl
CDR, 231st p

JOHN SMITH
CW4, Army
Special Agent In Charge

Figure I-13. CI applicant HRC memorandum

Appendix J

Unit Custodian Badge and Credentials Handbook

This handbook was prepared by the Badge and Credentials Program Management Office, INSCOM Training and Doctrine Support (ITRADS) Detachment, Fort Huachuca, AZ. The intent of the handbook is to provide unit-level custodians the current policies and administrative procedures required to effectively manage their unit accounts. Questions or comments concerning this handbook should be sent via Nonsecure Internet Protocol Router Network (NIPRNET) email to the ITRADS points of contact identified in this guide.

REFERENCE MATERIALS AND INFORMATION

J-1. **Reference materials.** This document contains the current policies and procedures for executing the basic badge and credentials actions required to effectively manage the unit's badge and credentials account. Please read and follow them. Future actions that do not comply with these instructions, guidelines, or requirements will be returned to the custodian without action. For now, custodians must have the following reference documents on file for inspection purposes. Once the new regulation is published these will be superseded:

- AR 381-20, U.S. Army Counterintelligence Activities, 15 November 1993.
- DAMI-CHI Memo, Subject: U.S. Army Intelligence (USAI) Badge and Credentials Hand-carry Guidance, 8 February 2001.
- DAMI-CDC Memo, Subject: Appropriate Display of USAI Badge and Credentials representative credentials, representative credentials, 15 March 2002.
- ITRADS Memo, Subject: The CI Badge Plaque and Trophy Program, 29 April 2005.

J-2. **ITRADS points of contact.** ITRADS is a small INSCOM Detachment on Fort Huachuca responsible for managing the Army's Badge and Credentials Program and maintaining the Army's Central Badge and Credentials Repository.

J-3. **Badge and credentials material description.** The term "badge and credentials materials" includes one or all of the following:

- **Military intelligence badge.** The MI badge has a control number stamped into the back; this is the number custodians report on receipts and inventories.
- **Intelligence credentials.** DA Forms 3363, 3363A, or 3363-1. Each form has a six-digit control number printed on the reverse side of the card; this is the number custodians will report on all receipts and inventories.

MUTUAL SUPPORT UNDERSTANDING AND AGREEMENT

J-4. ITRADS will work with the appointed unit custodians under a mutual support agreement or understanding. The agreement is based on the concept of support from support—meaning simply that ITRADS will support the unit custodian if the unit custodian supports ITRADS.

J-5. When a unit needs badge and credentials material support from ITRADS (badge and credentials, representative credentials, information), we will do our best to ensure the requirement is supported in a

timely manner. If for some reason ITRADS is going to be delayed in shipping your items or answering a question, ITRADS will send you an email with the details so that you know we are working the issue.

J-6. The same holds true when ITRADS needs support from a unit custodian (information requests, inventories, receipts); the expectation is that custodians will do their best to support the ITRADS requirement in a timely manner. ITRADS expects that if the custodian is going to be delayed in supporting an ITRADS requirement, the custodian would send ITRADS an email with the details so that we know you are working the issue.

J-7. The request process (how ITRADS does business): the program coordinator receives a properly formatted request before 1100 Arizona time; pulls or fabricates badge and credentials or representative credentials; documents the action; packages the items; then takes them to the mailroom by 1300. The ITRADS deadline to the installation mailroom is 1300, the custodian's deadline for getting requests to ITRADS is "before 1100 hours Arizona time"; this allows the program coordinator sufficient time to support your requirement with same-day service.

Note. ITRADS will not hold onto badge and credentials actions if they arrive after 1100 hours. If you know your request is not going to make it by the deadline for that day, please hold off and send it the following morning. Requests arriving after the established deadline will not be acted on. If there is a problem with your request, ITRADS will notify you of what the problems are, and expect you to make the necessary corrections and re-submit before 1100 Arizona time. Please take your time zone into consideration when sending requests to ITRADS.

J-8. The key to success in managing the account is to make sure our offices stay in routine email communication with each other. Custodians have a requirement to let this office know when all of the custodians will be out of the office or unit at the same time (for example, deployed, schools, TDY). This notification helps to prevent situations where ITRADS is left to wonder why you are not answering emails; it also reduces the frustration level.

J-9. Army intelligence badge and credentials and representative credentials are sensitive items that are accountable Army property; just like any other piece of accountable property within the organization, they will be controlled and accounted for at all times using a receipt and inventory system.

FUNDAMENTAL RULES AND GUIDELINES

J-10. Custodians are required to—

- Implement a suspense system for tracking and receipting for inbound badge and credentials materials, whether shipped or hand-carried to the unit.
- Receipt for badge and credentials materials, by badge and credentials control numbers, on the same day the badge and credentials materials arrive at the unit, whether shipped to the unit or hand-carried during reassignment.
- Coordinate hand-carry transfers, regardless of whether the agent wants to hand-carry, when the agent is being reassigned to a unit listed on the account custodian list.
- Inventory all unit badge and credentials materials semiannually and when the unit's primary custodians change.
- Retain all serviceable badge and credentials and representative credentials cases for badge and credentials materials returned to ITRADS. Unserviceable cases should be cut in half and thrown away.

J-11. Badge and credentials materials must be requested using the format provided by ITRADS.

J-12. Email is the easiest and most preferred method of sending a receipt. Signed receipts may be faxed to ITRADS, provided the custodian verifies the fax arrival at ITRADS either by phone or email. Agents will not hand-carry badge and credentials without written (email) authorization from ITRADS.

J-13. When agents are not authorized to hand-carry their badge and credentials, or when they are separated from Army service, the unit custodian is required to ship that agent's badge and credentials back to ITRADS as soon as the agent no longer needs their badge and credentials (for example, when the agent out-processes through the custodian).

J-14. Requirements when addressing emails:

- When a custodian sends a badge and credentials-related email to ITRADS, the email must be addressed to the badge and credentials PM and coordinator, as well as all the other appointed custodians from their own unit.
- When a custodian sends a badge and credentials-related email to another unit, the email must be addressed to all of the appointed units for the other unit, the badge and credentials PM and coordinator from ITRADS, as well as all of the other appointed custodians from their own unit.

RECEIPT FOR BADGE AND CREDENTIALS MATERIALS

J-15. ITRADS is still expending an inordinate amount of time having to ask custodians for receipts. Future emails from ITRADS asking for overdue receipts will be addressed directly to the account holder, with a courtesy copy to the custodian.

J-16. Baseline receipt requirements:

- **Badge and credentials materials shipped to the unit**—Custodians are required to receive, inventory, inspect, and receipt for those items on the same-day the package is delivered to your unit. Establishing a good working relationship with the unit's mailroom personnel is one way to ensure you are aware when a package arrives.
- **CONUS custodians—**When ITRADS ships you a package, it will be through Federal Express. ITRADS will send you an email indicating that the package has been shipped; you should be looking for that package the next day. Figure J-1 is an example of an email receipt for badge and credentials materials shipped to a unit.

TO: (b&coffice@hua.army.mil); (randall.long@hua.army.mil)
CC: (All gaining unit custodians, other than sending custodian)
SUBJECT: Receipt for Badge and Credentials Materials

I have inventoried and assume responsibility for the following items: *(list all items that apply)*

SGT DOE, John J. *(Note: include rank and name if badge and credentials/representative credentials are mailed as a set.)*
Badge: 12345
DA 3363: 03-1234
DA 3363-1: 03-4321
- or –
Representative Credentials: R-4000
DA 3363A: 03-1234
DA 3363-1: 03-4321

Figure J-1. Email receipt for badge and credentials materials shipped to a unit

Note. The program coordinator provides same-day processing and shipping of badge and credentials materials, provided he receives a complete, accurate request by 1100 hours Arizona time. If you are unable to meet this deadline, please forward your request first thing the next morning.

- **CI badge and credentials hand-carried to the unit**—Custodians are required to inventory, inspect, and receipt for hand-carried badge and credentials, on or before the agent's report date into the unit, depending on whether or not the agent signs in earlier than the scheduled report date. The easiest way to track inbound hand-carry actions is to write the inbound agent's name on your desk calendar, on the agent's report date; this method will allow you to know immediately when you should be looking for an inbound set of badge and credentials. Another recommendation is to put a separate requirement on the unit's in and out-processing checklist requiring all newly assigned CI personnel (35L, 351L, 35E, Army Civilians, and Military Intelligence Excepted Career Program [MICECPs]) to in/out-process through the account custodian. Figure J-2 is an example of an email receipt for CI badge and credentials hand-carried to the unit.

TO: (All of the losing unit custodians)
CC: b&coffice@hua.army.mil; randall.long@hua.army.mil; (All of the gaining unit custodians, other than the sending custodian)
SUBJECT: Receipt for Hand-Carried Badge and Credentials

I have inventoried and assume responsibility for the following badge and credentials:
SGT DOE, John J
Badge: 12345
DA 3363: 03-1234
DA 3363-1: 03-4321

Figure J-2. Email receipt for CI badge and credentials hand-carried to a unit

J-17. **Transmission and format.** The easiest and most preferred method of sending a receipt for badge and credentials materials is using unclassified email. When ITRADS receives an email receipt, the custodian will get an email "thanks" back from ITRADS to confirm receiving the email receipt. Custodians should print all email receipts they receive from ITRADS or other unit custodians as proof of the receipt action. All receipts are to be maintained on file until the next unit inventory is reconciled with ITRADS.

J-18. **Faxing receipts.** Hardcopy receipts may be faxed to ITRADS provided the receipt reaches ITRADS on the same day the badge and credentials materials arrived at the unit. It is the responsibility of the unit custodian to follow-up on all documents faxed to ITRADS to ensure they were received.

J-19. **Mailing receipts.** Receipts cannot be mailed; this method of receipting for badge and credentials materials does not comply with the same-day receipt requirement.

HAND-CARRY TRANSFER POLICY AND COORDINATION PROCESS

J-20. Custodian definitions:

- **Losing unit custodians.** Custodians for the unit the agent is currently assigned to.
- **Gaining unit custodians.** Custodians for the unit the agent is being reassigned to.

J-21. **Army policy.** The Army may authorize agents to hand-carry, or physically take their CI badge and credentials during reassignments for the purpose of eliminating the agent's downtime at the gaining unit and to reduce postal expenses across the Army. Hand-carry transfers must be formally coordinated in

accordance with the policies and procedures provided below. There are no "informally" coordinated hand-carry transfers.

- CI special agents will not PCS with badge and credentials without written authorization (email) from ITRADS.
- Hand-carry transfers must be coordinated if the agent is being reassigned to a unit that has an established badge and credentials account, and will be coordinated not earlier than 30 days out from the day the agent physically departs the unit. Hand-carry transfers will not be approved for agents who are being reassigned to a unit that does not appear on the account custodian list, which means the unit doesn't have a badge and credentials account.
- Agents do not have a choice whether they hand-carry their badge and credentials during reassignment. The hand-carry decision will be made during coordination between the custodians involved and ITRADS.

Note. If there are extenuating personal circumstances which may impact the agent's hand-carry, the unit custodian must bring it to the attention of ITRADS immediately. Depending on the situation, ITRADS may direct the losing unit to ship the agent's badge and credentials directly to the gaining unit's custodian.

- Hand-carry transfers will not be approved for agents who are attending a school, or who are going to be TDY in route.
- The gaining unit is not authorized to initiate the hand-carry email process; only the losing unit's custodians may initiate the hand-carry email coordination process.
- Badge and credentials stay on the losing unit's inventory until the gaining unit's custodian sends a receipt to the losing unit's custodians, and ITRADS. Therefore, if the losing unit sends an inventory to ITRADS before receiving a receipt from the gaining unit for the hand-carried badge and credentials, the hand-carried badge and credentials must still be included on the losing unit's inventory.
- There are no "informally" coordinated hand-carry transfers, all initial hand-carry emails must be formatted and addressed in accordance with the following ITRADS guidance.

J-22. **Hand-carry transfer email coordination process.** The entire effort to coordinate the hand-carry of CI badge and credentials involves a total of five emails: one from the losing unit, two from the gaining unit, and two from ITRADS. Hopefully custodians will realize that coordinating a hand-carry transfer is much easier than packaging up badge and credentials for shipment back to ITRADS or to another unit. Figures J-3 through J-7 (pages J-6 through J-8) provide examples of what the string of emails would look like for a properly coordinated hand-carry transfer with receipt and acknowledgment.

Note. If the initial hand-carry email is addressed properly, custodians can simply use the "Reply to all" button when responding.

- The first email is sent from the losing unit's custodian to all the gaining unit custodians and ITRADS. The email simply notifies everyone involved that an agent is on orders to an organization that has a badge and credentials account. The initial email must contain the following:

The following individual is being reassigned to (gaining unit).
Are badge and credentials required upon arrival?
Rank/Name: *(SGT Doe, John J.)*
Badge Number: *(12345)*
Report Date: *(XX Jan 03)*

- The second email is the gaining unit custodian's reply to the initial email, which is addressed back to the losing unit's custodians and ITRADS. This email is the gaining unit's custodian's answer to the question "are badge and credentials required upon arrival." If the answer is no, the custodian will request the agent's badge and credentials be sent back to ITRADS. If the answer is yes, the custodian will also ask for hand-carry authorization. The reply to the initial email must contain one of the following responses:

No, badge and credentials are not required upon arrival; please return them to ITRADS.
Yes, badge and credentials are required upon arrival; request hand-carry authorization.

- The third email is sent from ITRADS and will either approve or disapprove the hand-carry. If the first two emails are properly coordinated, ITRADS will send the following hand-carry authorization:

SGT Doe is authorized to hand-carry badge and credentials from (losing unit) to (gaining unit).

- The fourth email is the gaining unit custodian's receipt for the badge and credentials, and must be addressed to all of the custodians from the losing and gaining units and ITRADS. The email will provide all required receipt information, which includes the credential's control numbers.

I have inventoried and assume responsibility for the following badge and credentials:
SGT DOE, John J.
Badge: *(12345)*
DA 3363: *(03-1234)*
DA 3363-1: *(03-4321)*

- The fifth and final email is sent by ITRADS. Upon receipt of the gaining unit's email receipt, ITRADS will send a simple "Thanks" replying to all of the custodians for the losing and gaining units. By doing so, ITRADS officially acknowledges the transfer of badge and credentials from the losing unit's to the gaining unit's inventory.
- Figures J-3 through J-7 provide examples of what the five emails will look like when a hand-carry transfer is properly coordinated between the losing and gaining units, and approved by ITRADS.

Email 1—The Losing Unit Initiates the Hand-Carry Coordination: This email is the initial notification to the gaining unit and ITRADS that an agent is being reassigned to a unit that has an established badge and credentials account. This email is sent from the losing unit's custodian to the gaining unit's custodians and ITRADS.
FM: (A losing unit custodian)
TO: (All of the gaining unit's custodians)
CC: (All of the losing unit's custodians, except the sender); badge and credentials Program Manager and Coordinator
SUBJECT: Hand-carry Transfer
The following individual is being reassigned to the (gaining unit).
Are badge and credentials required upon arrival?
Rank, Full Name: SGT Doe, John J.
Badge Number:12345
Report Date: XX Jan 03

Figure J-3. Email 1 example—hand-carry transfer coordination process

Email 2—The Gaining Unit Responds to the Initial Email: The gaining unit's custodian responds to the initial hand-carry coordination email, providing a determination as to whether the agent will require badge and credentials upon arrival at the gaining unit and, if so, requests authorization for the hand-carry. This email is sent to the losing unit's custodians and ITRADS.

FM: (A gaining unit custodian)

TO: (All of the losing unit's custodians)

CC: (All of the gaining unit's custodians, except the sender); badge and credentials Program Manager and Coordinator

SUBJECT: Hand-Carry Transfer

Badge and credentials will be required upon arrival; request authorization for hand-carry.

Figure J-4. Email 2 example—gaining unit responds to the initial email

Email 3—The Hand-Carry Authorization Email from ITRADS:

FM: (ITRADS)

TO: (All of the losing unit's custodians)

CC: (All of the gaining unit's custodians); Badge and Credentials Program Manager and Coordinator

SUBJECT: Hand-Carry Transfer

SGT Doe is authorized to hand-carry badge and credentials from (losing unit) to (gaining unit).

Figure J-5. Email 3 example—hand-carry authorization email from ITRADS

Email 4—The Gaining Unit Receipts for the Badge and Credentials: This email is sent from the gaining unit's custodian to the losing unit custodians and ITRADS, and is required to be sent on the same day that the agent arrives at the unit. This is the basic email receipt for CI badge and credentials hand-carried to a unit.

FM: (A gaining unit custodian)

TO: (All of the losing unit's custodians)

CC: (All of the gaining unit's custodians, except the sender); badge and credentials Program Manager and Coordinator

SUBJECT: Receipt for Hand-Carried Badge and Credentials

I have inventoried and assume responsibility for the following badge and credentials:

SGT DOE, John J

Badge: 12345

DA 3363: 03-1234

DA 3363-1: 03-4321

Figure J-6. Email 4 example—gaining unit receipts for the badge and credentials

Email 5—ITRADS Acknowledgment of Transfer: This email is sent as a reply to the gaining unit's receipt email, and is a simple "Thanks" to let both unit's custodians know that ITRADS acknowledges the official transfer of badge and credentials from the losing to the gaining unit's inventory.

FM: (ITRADS)

TO: (All of the gaining unit's custodians)

CC: (All of the losing unit's custodians); Badge and Credentials Program Manager and Coordinator

SUBJECT: Receipt for Hand-Carried Badge and Credentials

Thanks

Figure J-7. Email 5 example—ITRADS acknowledgment of transfer

INVENTORIES

J-23. Custodians are required to conduct a 100 percent hands-on physical inspection and inventory of all badge and credentials materials issued to the unit's account, semiannually and when the unit's primary custodian changes.

J-24. Semiannual inventories must be conducted every six months during the month and year identified in the latest ITRADS inventory reconciliation memorandum or email.

J-25. Change of custodian inventories are more involved; they require that a joint inventory be conducted between the incoming and outgoing primary custodians. This joint inventory must be conducted and reconciled with ITRADS before the physical departure of the outgoing primary custodian, and must be signed by both the incoming and outgoing primary custodians.

J-26. Custodians may not conduct an inventory using on-hand receipts. When an individual issued badge and credentials materials is not present for an inventory (for example, deployment, extended TDY), the custodian will contact that individual or another responsible person who can verify that the individual still has the items in their possession, and to confirm all appropriate control numbers to the custodian.

J-27. Inventories must be prepared in a roster (column) format, alphabetically, with separate columns for the agent's name, rank, badge number, 3363, 3363A and 3363-1 numbers. If the unit is not responsible for representative credentials then there will be no requirement for a 3363A column. Do not include social security numbers (SSNs) on inventories.

J-28. All inventories faxed to ITRADS must be signed by the custodian who conducted the inventory.

J-29. Because of the signature requirement for change of custodian inventories, they must be faxed to ITRADS. The signed inventory may be scanned and saved as a .pdf document (Adobe Acrobat readable), and sent to ITRADS as an attachment to an email, provided ITRADS can open the document.

J-30. When badge and credentials materials are transferred to another unit's account or returned to ITRADS, those items remain on the losing unit's inventory until the gaining unit's custodians or ITRADS receipts for the items.

J-31. The physical inspection of the badge and credentials materials is to ensure the badge is not worn, tarnished, or excessively bent. The credential forms will be inspected to ensure the lamination is not splitting or they are excessively scratched.

J-32. The unit's inventory will be compared against the Army's Central Badge and Credentials Repository database. Once the inventory is reconciled, ITRADS will send an email to the unit custodian confirming the reconciliation. The email will provide the month and year the unit's next semiannual inventory is due, and directs the custodian to print the inventory reconciliation email as the unit's official inventory reconciliation documentation. This email is required to be maintained on file by the unit until the next semiannual or change of custodian inventory is reconciled.

J-33. Figure J-8 is an example of a unit badge and credentials inventory memorandum format.

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(***Unit's Office Symbol***) (***Today's Date***)

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (Badge and Credentials), 2520 HEALY STREET, FT HUACHUCA, AZ 85613-7050

SUBJECT: USAI Badge and Credentials Program - Account Inventory

1. Reference AR 381-20, The Army CI Program, 5 November 1993.

2. On (*date*) the undersigned conducted a physical 100 percent hands-on inventory and inspection of all badge and credentials materials for which this organization is accountable. All badge and credentials forms listed below have been physically inspected and are in serviceable condition.

RANK	***NAME***	***NUMBER***	***DA 3363/A***	***DA 3363-1***
PFC	Atlanta, George G. II	1111	03-111	03-0000
LTC	Baltimore-Washington, Mary L.	R-4444	02-1958	02-8591
CW3	El Paso, TX S. Jr.	12345	99-0009	98-1234
GG-13	Monterey, CA O. Sr.	R-1234	99-9000	98-4321

INSTRUCTIONS: List the individual's rank, full name (Last, First, MI, suffix), the MI badge or representative credential number, the DA Form 3363 or 3363A number, and finally the DA Form 3363-1 number. The credential control numbers are printed on the back of the credential forms, a 6-digit number. Inventories must be prepared alphabetically by last name. Do not include any other information on this memorandum; do not list items as deployed, on-hand, TDY, or other. This inventory will be a complete list of every item (badge and credentials and/or representative credentials) for which your unit is accountable.

3. Questions concerning this inventory should be directed to the undersigned at **(*custodian contact information, phone, DSN, email).***

CUSTODIAN
OFFICIAL SIGNATURE BLOCK

Note. Signed inventories can be faxed to ITRADS, or scanned and attached to an email to ITRADS. Once ITRADS' reconciles the inventory - an inventory reconciliation email is sent to the unit custodian - the email will confirm inventory reconciliation and identify the month and year the next semiannual inventory is due.

Figure J-8. Unit badge and credentials inventory memorandum format

RECEIPT AND RESPONSIBILITY STATEMENTS

J-34. Custodians must have a signed and dated receipt and responsibility statement on file for each set of CI badge and credentials and representative credentials issued to unit personnel. Figure J-9 provides an electronic format to be used by custodians to internally receipt for badge and credentials materials.

J-35. Custodians must provide a receipt to those individuals who surrender their badge and credentials or representative credentials to the custodian. Once an individual has been provided a receipt for their badge and credentials or representative credentials, any old Receipt and Responsibility Statements for that individual should be destroyed. In other words, do not keep old receipts from individuals who no longer have possession of their badge and credentials or representative credentials.

J-36. Custodians who have issued badge and credentials or representative credentials to individuals for extended use, should require those individuals to review, initial, and date both the responsibility statement and receipt every time an inventory is conducted.

J-37. The responsibility statement is designed to be used by a commander, as supporting documentation for AR 15-6 investigations, in the event an individual misuses or loses their CI badge and credentials or representative credentials.

RESPONSIBILITY STATEMENT

(This form will be used for both Badge and Credentials and Representative Credentials.)

Initials of Individual

____I understand that the badge and credentials or representative credentials identified below are the property of the Army and are issued to me based on a mission that requires me to identify myself as a duly accredited CI special agent (badge and credentials) or representative of Army Intelligence (representative credentials).

_____I will only display my badge and credentials or representative credentials when I am required to identify myself as a duly accredited CI special agent or representative of Army Intelligence.

_____I understand that misuse will have occurred if I display my badge and credentials or representative credentials for any other reason than to identify myself as a CI special agent or representative of Army Intelligence who is conducting an authorized CI investigative or intelligence-related activity.

_____I understand that, should I witness the misuse of badge and credentials or representative credentials, I am required to report the incident immediately to the unit badge and credentials custodian or account holder, who is either the Commander or C/J/G/S-2.

_____I understand that I am solely responsible for safeguarding my badge and credentials or representative credentials to prevent their loss or theft, regardless of my duty location.

_____I understand that should my badge and credentials or representative credentials become lost, I am responsible for reporting the loss to my immediate supervisor, the unit badge and credentials custodian, and commander, and that I will continue to search for these items until found or officially relieved from searching.

_____I understand that I am responsible for becoming familiar with the provisions of AR 381-20, chapter 9, the supplemental policy guidance issued by ITRADS, as well as all organizational level policies and procedures for controlling and accounting for badge and credentials and representative credentials.

_____Badge and Credentials Holders Only: I understand that I must receive an approval from ITRADS before I can PCS with my badge and credentials, and to receive the approval, I must notify my unit badge and credentials custodian in sufficient time to allow for the proper coordination of the transfer.

RECEIPT STATEMENT

The undersigned assumes responsibility for the following set of U.S. Army Intelligence Badge and Credentials or Representative Credentials:

Badge and Credentials:

Badge Number: _____
DA Form 3363: _____
DA Form 3363-1:_____
Representative Credentials:_____
DA Form 3363A:_____

Signature: _____
Printed Name:_____
Receipt Date: _____

Figure J-9. Receipt and responsibility statement format

RETURNING BADGE AND CREDENTIALS MATERIALS TO ITRADS

J-38. The baseline requirement for custodians to return badge and credentials materials is that badge and credentials materials will be expeditiously returned to ITRADS when they are no longer required.

- For representative credentials, they will be retrieved by the custodian and returned to ITRADS when the individual to whom they were issued is reassigned or is removed from the duties or mission that required the representative credentials. Once the mission for which the representative credentials were issued ends, the representative credentials will not be retained at the unit for future issue. representative credentials are not transferable between units.
- For CI badge and credentials, they will be retrieved by the custodian and returned to ITRADS when the agent is being reassigned and not authorized to hand-carry; the custodian should retrieve these badge and credentials during the agent's out-processing and return them. Custodians will also expeditiously return badge and credentials for agents who have had their clearance formally suspended or revoked.

J-39. Custodians must include orders for all CI badge and credentials being returned to ITRADS. If badge and credentials materials are returned for reasons or situations for which orders are not generated, custodians will annotate on the return memorandum why the badge and credentials materials are being returned.

J-40. Custodians are ultimately responsible for ensuring that badge and credentials materials are shipped using one of the following postal services (Federal Express, Registered, or Postal Express). This is Army policy; custodians must ensure their unit mailrooms understand this requirement. Noncompliance with this requirement will be addressed to the unit's account holder for command involvement.

J-41. Custodians must include a receipt in all packages of badge and credentials shipped to ITRADS or another unit. The receipt will be an itemized list of all items within the package. Figure J-10 is an example of a badge and credentials return memorandum format.

J-42. Upon receiving the badge and credentials materials, ITRADS will normally send the custodian an email receipt for the items. In the event ITRADS receives a large shipment of badge and credentials materials, the hardcopy receipt may be faxed back to the unit custodian.

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(Unit's Office Symbol) ***(Today's Date)***

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (Badge and Credentials), RM 1279, BLDG 51005,
2520 HEALY STREET, FT HUACHUCA, AZ 85613-7050

SUBJECT: Return of US Army Intelligence Badge and Credentials Materials

1. Reference AR 381-20, The Army CI Program, 15 November 1993.

The following (badge and credentials and/or representative credentials) are being returned to ITRADS:

GRADE	***NAME***	***BADGE/RC#***	***DA 3363/A***	***DA 3363/1***	***REASON***
PFC	Doe, John L.	02-1234	02-1234	02-4321	PCS, ETS
GG-13	Smith, Elmo A.	R-4000	02-4321	02-1234	Retire

ORDERS REQUIREMENT: When you send badge and credentials back to ITRADS for agents who have PCS'd or separated from Army service (Chapter, ETS, Retirement, Resignation), you are required to provide ITRADS with a copy of that agent's orders. Orders are not required when returning representative credentials.

2. POC for this action is (your unclassified email address, telephone, unclassified and DSN number).

UNIT BADGE AND CREDENTIALS CUSTODIAN
(Primary or Alternate)
SPECIAL SIGNATURE BLOCK

RECEIPT STATEMENT

Receipt Statement: ITRADS has received the items above and removed them from your inventory.

Name: Signature:

Date Received:

Note. ITRADS will normally send an email receipt to custodians for badge and credentials materials returned to ITRADS. Custodians should print the ITRADS email receipt and maintain it on file.

Figure J-10. Example of badge and credentials return memorandum format

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(Unit's Office Symbol) ***(Today's Date)***

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (Badge and Credentials), RM 1279, BLDG 51005, 2520 HEALY STREET, FT HUACHUCA, AZ 85613-7050

SUBJECT: Request for US Army CI Badge and Credentials

1. Request counterintelligence (CI) badge and credentials be issued to this unit for the following agent(s): *(Custodians requiring multiple sets of CI badge and credentials should include all of the required information, for each agent, on this one memorandum.)*

Name: **(Last Name, First Name, Middle Initial - if no middle initial, type NMI)**
Grade: **(Military E-?, W-?, O-?, and for Civilians GG-12, GG-13)**
SSN: **(Self-Explanatory)**
MOS/Series: **(Military—35L, 351B, 35E, Civilian Series - 0132)**
Component: **(Active, Reserve, Guard, DAC or MICECP)**
Birth date: **(Date of birth only—use this format: 30 Dec 58)**
Clearance: (**TS, Interim TS—See Note in paragraph 2)**
Date Clearance Granted: **(From JPAS [Joint Personnel Adjudication System])**

2. The above named individual(s) requires CI badge and credentials for the following missions:

a. In this paragraph custodians are required to list the CI Special Agent's current duty position and describe the specific CI missions and duties associated with that duty position that require the use of CI badge and credentials.

b. This paragraph will also include a statement on the adverse impact not having badge and credentials will have on the unit's mission, specifically what part of the Agent's assigned CI missions will they not be able to perform if they do not have CI badge and credentials for identification.

Note. By regulation CI Special Agents are required to have a Final TS clearance. If you are requesting CI badge and credentials for an agent that only has an Interim TS clearance, then your memorandum must be submitted as a request for exception to policy.

3. POC for this action is (your unclassified email address, telephone, unclassified fax and DSN).

UNIT BADGE AND CREDENTIALS CUSTODIAN
(Primary or Alternate)
SPECIAL SIGNATURE BLOCK

Figure J-11. Badge and credentials request memorandum format

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(Unit's Office Symbol) ***(Today's Date)***

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (Badge and Credentials), RM 1279, BLDG 51005, 2520 HEALY STREET, FT HUACHUCA, AZ 85613-7050

SUBJECT: Request for US Army Intelligence Representative Credentials

1. Request US Army Intelligence Representative Credentials be issued to this organization for the following named individual: *(Commanders may request representative credentials for multiple individuals using this one request memorandum provided all of the following information is provided for each individual requiring representative credentials.)*

Name: ***(Last, First, Middle Initial)***
Grade: ***(Military E-?, W-?, O-?, and for Civilians GG-12, GG-13)***
SSN: ***(Self-Explanatory)***
MOS/Series: ***(97E, 351E, 0132, etc.)***
Component: ***(Active, Reserve, Guard, DAC, MICECP)***
Birth date: ***(Date of birth only—example: 30 Dec 58)***
Clearance Level: ***(Secret, TS)***
Date Clearance Granted: ***(From DA 873 - example: 30 Dec 98)***
Length of Mission: ***(From Month/Year To Month/Year)***
Mission Requirement for Representative Credentials: The above-named individual will be conducting the following missions which require the use of representative credentials: (*Be specific. The requirement is to provide the individual's current position and describe those specific duties the individual will be conducting that require the use of representative credentials. Describe the adverse impact not having these representative credentials will have on the unit's mission.)*

2. POC for this action is *(the preparing custodian's rank, name, unclassified email address, telephone, unclassified fax and DSN number).*

ACCOUNT HOLDER
OFFICIAL SIGNATURE BLOCK

Figure J-12. Request for USAI representative credentials

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(Unit's Office Symbol) ***(Today's Date)***

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (Badge and Credentials), 2520 HEALY STREET, FT HUACHUCA, AZ 85613-7050

SUBJECT: Misuse of US Army Intelligence Badge and Credentials - Initial Report

1. Circumstances of Misuse:

a. Individual Involved: *(Rank, name of the individual who misused the badge and credentials).*

b. badge and credentials Involved: *(Badge number and credential control numbers of items).*

c. Misuse Allegations: *(A brief description of the misuse allegations).*

2. On *(date)*, an AR 15-6 investigation for misuse of badge and credentials was initiated by *(rank and name)* who appointed *(rank and name)* as the investigating officer. Upon completion of the AR 15-6, a final Report of Misuse will be forwarded that provides a summary of the investigative results.

3. Point of contact for this Report is *(Primary custodian's rank and name, commercial and DSN telephone numbers, and unclassified email address).*

ACCOUNT HOLDER (Commander or C/J/G/S-2)
OFFICIAL SIGNATURE BLOCK

Note. If this Report is being submitted for misuse of representative credentials, make the appropriate substitutions throughout the Report.

Figure J-13. Misuse of badge and credentials materials—initial report format

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(Unit's Office Symbol) ***(Today's Date)***

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (Badge and Credentials), 2520 HEALY ST., FT HUACHUCA, AZ 85613-7050

SUBJECT: Misuse of US Army Intelligence Badge and Credentials - Final Report

1. The AR 15-6 investigation into the misuse of badge and credentials by (rank and name) was completed on (date). The investigating officer (rank and name) determined that the allegations of misuse were (substantiated or unsubstantiated). This determination was based on the following investigative results:

a. *(List results.)*
b. *(List results.)*

2. Based on the results of this investigation and the investigating officer's recommendations, the commander has taken the following actions: *(Include all disciplinary or administrative actions taken along with any action to remove the individual from the CI Program.)*

3. Point of contact for this Report is *(Primary custodian's rank and name, commercial and DSN telephone numbers, and unclassified email address).*

ACCOUNT HOLDER (Commander or C/J/G/S-2)
OFFICIAL SIGNATURE BLOCK

Note. If this Report is being submitted for misuse of representative credentials, make the appropriate substitutions throughout the Report.

Figure J-14. Misuse of badge and credentials materials—final report format

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(Unit's Office Symbol) ***(Today's Date)***

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (Badge and Credentials), 2520 HEALY STREET, FT HUACHUCA, AZ 85613-7050

SUBJECT: Loss of US Army Intelligence Badge and Credentials - Initial Report

1. Circumstances of Loss:

a. Individual(s) Involved: *(Rank, name of the individual who lost the badge and credentials)*
b. Lost Items - **Badge#:** **DA Form 3363:** **DA Form 3363-1:**
c. Incident Description: *(Provide a brief description of how the items were lost.)*

2. Actions taken to date:

a. Upon discovery of loss this organization conducted an immediate recovery search for the missing items, notified the badge and credentials Program Office immediately and made *(list the local, state, and national agencies notified)* aware of the missing items and requested their assistance.
b. On *(date)*, an AR 15-6 investigation for loss of badge and credentials was initiated by *(rank and name)* who appointed *(rank and name)* as the investigating officer. Upon completion of the AR 15-6, a final Report of loss will be forwarded that summarizes the investigative results.

3. Point of contact for this Report is *(Primary custodian's rank and name, commercial and DSN telephone numbers, and unclassified email address).*

ACCOUNT HOLDER (Commander or C/J/G/S-2)
OFFICIAL SIGNATURE BLOCK

Note. If this Report is being submitted for loss of representative credentials, make the appropriate substitutions throughout the Report.

Figure J-15. Loss of badge and credentials materials—initial report format

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(Unit's Office Symbol) ***(Today's Date)***

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (badge and credentials), RM 1279, BLDG 51005, 2520 HEALY STREET, FT HUACHUCA, AZ 85613-7050

SUBJECT: Loss of US Army Intelligence Badge and Credentials - Final Report

1. The AR 15-6 investigation into the loss of badge and credentials by (rank and name) was completed on (date). The investigating officer (rank and name) determined that the loss of these items (was/was not) due to negligence on the part of the (custodian, agent, mailroom personnel, other). This determination was based on the following investigative results:

a. *(List results.)*
b. *(List results.)*

2. Request relief from accountability for the following items:

Badge: **DA Form 3363:** **DA Form 3363-1:**

3. Based on the results of this investigation and the investigating officer's recommendations, the commander has taken the following actions: (*Include all disciplinary or administrative action taken along with any action to remove the individual from the CI Program.)*

4. Point of contact for this Report is *(Primary custodian's rank and name, commercial and DSN telephone numbers, and unclassified email address).*

ACCOUNT HOLDER (Commander or C/J/G/S-2)
OFFICIAL SIGNATURE BLOCK

Note. If this Report is being submitted for loss of representative credentials, make the appropriate substitutions throughout the Report.

Figure J-16. Loss of badge and credentials materials—final report format

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

REPLY TO
ATTENTION OF:

(Office Symbol) ***(Today's Date)***

MEMORANDUM FOR RECORD

SUBJECT: Additional Duty Appointment - Badge and Credentials Custodians

1. Effective ***(dd mm yy)***, the following individuals are appointed as the ***(Organization)*** Primary and Alternate Badge and Credentials Custodians:

a. Primary Custodian:
(1) Full name: *Public, John Q.*
(2) Grade/MOS: *O3, 35E*
(3) NIPRNET email address: *John.Public@installation.army.mil*
(4) SIPRNET email address: *John.Public@installation.army.smil.mil*
(5) Telephone numbers:
(a) Commercial and DSN:
(b) Unclassified fax:

b. Alternate Custodian(s):
(1) Full name: *Public, John Q.*
(2) Grade/MOS: *O3, 35E*
(3) NIPRNET email address: *John.Public@installation.army.mil*
(4) SIPRNET email address: *John.Public@installation.army.smil.mil*
(5) Telephone numbers:
(a) Commercial and DSN:
(b) Unclassified fax:

2. Authority: Army Regulation 381-20, chapter 9, paragraph 9-2c(1), dated 15 November 1993.

3. Period: Until these orders are rescinded or until officially relieved from appointment.

4. Purpose: To manage the USAI Badge and Credentials account.

5. The POC for this action is ( ).

APPOINTING OFFICIAL
SIGNATURE BLOCK

Figure J-17. Additional duty appointment badge and credentials custodians

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(Office Symbol) ***(Today's Date)***

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (Badge and Credentials), FT HUACHUCA,
AZ 85613-7050

SUBJECT: Request to Establish a USAI Badge and Credential Account

1. Request a USAI badge and credentials account be established for **(Organization)**, in accordance with the provisions of AR 381-20, chapter 9. This organization will follow all established Army specific policies and procedures for controlling and accounting for Army badge and credentials.

2. **(Organization)** is currently authorized (Number) CI personnel who require badge and credentials to perform the authorized mission of this unit.

3. The authorized Army CI missions of this organization that require the use of Army badge and credentials, for identification purposes, are: **(List and describe in detail, at the unclassified level, all of the missions your agents are performing that require them to use badge and credentials.)**

4. The following unit personnel will be appointed on orders as this organization's Primary and Alternate badge and credentials' account Custodians:

a. Primary Custodian:
(1) Full name: *(Last, First, MI)*
(2) Grade/MOS:
(3) Commercial and DSN and fax telephone numbers:
(4) NIPRNET email address:
(5) SIPRNET email address:

b. Alternate Custodian: *(Follow format for any additional alternates if appointed on orders)*
(1) Full name: *(Last, First, MI)*
(2) Grade/MOS:
(3) Commercial and DSN and fax telephone numbers:
(4) NIPRNET email address:
(5) SIPRNET email address:

5. The official mailing addresses for this organization are:

Official Military:	Commercial Mail Address:
Cdr, 123rd MI Bn	***Cdr, 123rd MI Bn***
ATTN: ABCD-EF	***ATTN: ABCD-EF (Custodian's Name)***
Ft Huachuca, AZ 85613	***Rm 1234, Bldg 5678, 9012 Memorandum Dr***
	Sierra Vista, AZ 85635

Figure J-18. Request to establish a USAI badge and credentials account

(Office Symbol)

SUBJECT: Request to Establish a USAI Badge and Credential (Badge and Credentials) account

6. The undersigned and all subordinate commanders will ensure their CI and intelligence personnel are sufficiently trained on the Army's policies and procedures for controlling and accounting for their badge and credentials to protect against theft, loss, or misuse.

7. Questions or comments concerning this request should be directed to (Primary Custodian's Name) at (either the DSN or Commercial phone number).

COMMANDER/ACCOUNT HOLDER
OFFICIAL SIGNATURE BLOCK

Figure J-18. Request for revalidation of badge and credentials account (continued)

DEPARTMENT OF THE ARMY
Headquarters, Organization's Official Letterhead
Installation, State Zip

(Office Symbol) ***(Today's Date)***

MEMORANDUM FOR CDR, USAIC&FH, ATTN: IATD (Badge and Credentials), FT HUACHUCA, AZ 85613-7050

SUBJECT: Request for Revalidation of Badge and Credential Account

1. Request revalidation of this organization's requirement for a US Army badge and credentials account, in accordance with the provisions of AR 381-20, chapter 9, and supplemental Army policy.

2. Request this account be revalidated as a (normal or a contingency) account based on the following authorized CI missions of this organization. ***(List and describe each authorized mission and related duties in detail at the unclassified level.)***

3. This organization is currently responsible for providing custodial support to the following organizations: ***(List the units supported by the account and the amount of badge and credentials materials you manage for that unit; if this account only supports one unit then delete this paragraph.)***

4. The following individuals have been appointed on orders as this unit's Primary and Alternate Custodians:

a. Primary Custodian:
(1) Full name: *(Last, First, MI)*
(2) Grade/MOS:
(3) Commercial and DSN and fax telephone numbers:
(4) NIPRNET email address:
(5) SIPRNET email address:

b. Alternate Custodian: *(Follow format for any additional alternates if appointed on orders)*
(1) Full name: *(Last, First, MI)*
(2) Grade/MOS:
(3) Commercial and DSN and fax telephone numbers:
(4) NIPRNET email address:
(5) SIPRNET email address:

5. The official mailing addresses for this organization are:

Official Military:	Commercial Mail Address:
Cdr, 123 MI Bn	***Cdr, 123d MI Bn***
ATTN: ABCD-EF	***ATTN: ABCD-EF (Custodian's Name)***
Ft Huachuca, AZ 85613	***Rm 1234, Bldg 5678, 9012 Memorandum Dr***
	Sierra Vista, AZ 85635

Figure J-19. Request for revalidation of badge and credentials account

(Office Symbol) *(Today's Date)*

SUBJECT: Request for Revalidation of Badge and Credential Account

6. The undersigned and all subordinate commanders will ensure their CI and intelligence personnel are sufficiently trained on the Army's policies and procedures for controlling and accounting for their badge and credentials to protect against theft, loss, or misuse.

7. The point of contact for this request is ***(Primary Custodian's information).***

ACCOUNT HOLDER
OFFICIAL SIGNATURE BLOCK

Figure J-19. Request for revalidation of badge and credentials account (continued)

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

ACE	analysis and control element
ACIC	Army Counterintelligence Center
ACICA	Army Counterintelligence Coordinating Authority
AIT	Advanced Individual Training
AKA	also known as
AKO	Army Knowledge Online
AO	area of operations
AOC	area of concentration
AOR	area of responsibility
AR	Army regulation
ARIMS	Army Records Information Management System
ARNG	Army National Guard
art.	article
ASCC	Army Service component command
AT	antiterrorism
ATCICA	Army theater counterintelligence coordianting authority
AWOL	absent without leave
BCT	brigade combat team
bde	brigade
BEAR	bonus extension and retention
BFSB	battlefield surveillance brigade
bldg	building
BSD	basic source data
C&E	communication and electronics
C2	command and control
C-2X	combined 2X
CA	civil affairs
CCN	case control number
CD	compact disk
cdr	commander
CE	counterespionage
CFSO	counterintelligence force protection source operations
CI	counterintelligence
CI&S	counterintelligence and security
CIA	Central Intelligence Agency
CICA	counterintelligence coordinating authority

CICP	Counterintelligence Collection Program
CID	Criminal Investigation Division
CIDC	Criminal Investigation Division Command
CIJ	counterintelligence jurisdiction
CIPP	Counterintelligence Probationary Program
CISAC	Counterintelligence Special Agents Course
CISO	counterintelligence staff officer
CITA	counterintelligence threat analysis
CMO	civil-military operations
CMOC	civil-military operations center
CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations
COA	course of action
COMSEC	communications security
CONUS	continental United States
COTS	commercial-off-the-shelf technology
CSPE	counterintelligence scope polygraph examination
CT	counterterrorism
DA	Department of the Army
DAC	Department of the Army Civilian
DACAP	Department of the Army Cryptographic Access Program
DCGS-A	Distributed Common Ground System-Army
DCID	Director of Central Intelligence Directive
DCS	deputy chief of staff
DEROS	date estimated return from overseas
DHA	detainee holding area
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DLAB	Defense Language Aptitute Battery
DNA	deoxyribonucleic acid
DNI	Director of National Intelligence
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DOMEX	document and media exploitation
DOT	Department of the Treasury
DPOB	date and place of birth
DS	direct support

DSN	Defense Switched Network
DSO	defensive source operations
DSS	Defense Security Service
DTG	date-time group
DUSD	deputy under secretary of defense
EO	executive order
EEFI	essential element of friendly information
EPW	enemy prisoner of war
ERB	enlisted records brief
ETS	expiration of term of service
EW	electronic warfare
fax	facsimile
FBI	Federal Bureau of Investigation
FFI	full field investigation
FISS	foreign intelligence and security services
FM	field manual
FNU	first name unknown
FOIA	Freedom of Information Act
G-2X	division, corps, and Army Service component command 2X
GEOINT	geospatial intelligence
GHz	gigahertz
GPS	global positioning system
GS	general support
GSR	general support-reinforcing
HHC	headquarters and headquarters company
HN	host nation
HOC	human intelligence operations cell
HQ	headquarters
HQDA	Headquarters, Department of the Army
HUMINT	human intelligence
I&W	indications and warning
ICF	intelligence contingency funds
IG	inspector general
IIR	intelligence information report
IMFR	investigative memorandum for record
INSCOM	United States Army Intelligence and Security Command
IP	investigative plan
IPB	intelligence preparation of the battlefield
ISR	intelligence, surveillance, and reconnaissance
ITO	international terrorist organizations

ITRADS	Intelligence and Security Command Training and Doctrine Support Directorate
J-2X	joint 2X
JIDC	joint interrogation and debriefing center
JP	joint publication
JTF	joint task force
JTTF	joint terrorism task force
JWICS	Joint Worldwide Intelligence Communications System
LAC	local agency check
LCA	limited counterintelligence assessment
LCCN	local case control number
LEA	law enforcement agency
LEP	locally employed person
LHM	letterhead memorandum
LNO	liaison officer
LNU	last name unknown
MAC	military agency check
MDMP	military decisionmaking process
METT-TC	memomy aid for the mission variables: mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MFR	memorandum for record
MHz	megahertz
MI	military intelligence
MICECP	Military Intelligence Civilian Excepted Career Program
MILDEP	military department
MILPO	military personnel office
MOS	military occupational specialty
MP	military police
MPRJ	military personnel records jacket
MSC	major subordinate command
NAC	national agency check
NATO	North Atlantic Treaty Organization
NCIC	National Crime Information Center
NCO	noncommissioned officer
NFI	not further identified
NGO	nongovernmental organization
NIPRNET	Nonsecure Internet Protocol Router Network
NMN	no middle name
no.	number
NRO	National Reconnaissance Office

NSR	no significant response
OCONUS	outside continental United States
OFCO	offensive counterintelligence operations
OJT	on-the-job training
OMT	operational management team
ONCIX	Office of the National Counterintelligence Executive
OPCON	operational control
OPLAN	operation plan
OPM	Office of Personnel Management
OPORD	operation order
OPSEC	operations security
OSC	operations support cell
PAC	personnel and administration center
PAO	public affairs office
PCS	permanent change of station
PDA	personal data assistant
PI	preliminary inquiry
PMO	provost marshal office
POB	place of birth
POC	point of contact
POV	privately owned vehicle
POW	prisoner of war
PQCO	polygraph quality control office
PSYOP	psychological operations
QC	quality control
RFA	request for assistance
RFI	request for information
rm	room
ROI	report of investigation
ROTC	Reserve Officers Training Corps
RTP	research and technology protection
S-2X	brigade 2X
SALUTE	size, activity, location, unit, time, equipment
SAP	special access program
SBCT	Stryker brigade combat team
SCA	special category absentee
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SIA	standing investigative authority
SIGINT	signals intelligence

SIP	subject interview plan
SIPRNET	Secure Internet Protocol Router Network
SJA	staff judge advocate
SMU	special mission unit
SOFA	status of forces agreement
SOI	summary of information
SOP	standing operating procedure
SSBI	single-scope background investigation
SSN	social security number
SSO	special security office
TA	threat assessment
TCI	technical counterintelligence
TDY	temporary duty
TECHINT	technical intelligence
TFCICA	task force counterintelligence coordinating authority
TMO	technology management office
TSCM	technical surveillance countermeasures
TTP	tactics, techniques, and procedures
USC	United States Code
UCMJ	Uniform Code of Military Justice
U.S.	United States
USACIDC	United States Army Criminal Investigations Division Command
USAHRC	United States Army Human Resources Command
USAI	United States Army Intelligence
USAIC&FH	United States Army Intelligence Center and Fort Huachuca
USAIRR	United States Army Investigative Records Repository
VA	vulnerability assessment
v.	versus
WMD	weapon of mass destruction
WO	warrant officer

SECTION II – TERMS

2X

Denotes the 2X positions at all echelons. The counterintelligence and human intelligence advisor to the C/J/G/S-2. The 2X staff conducts technical control and oversight for all counterintelligence and human intelligence entities with their operational purview. It coordinates, de-conflicts, and synchronizes all counterintelligence and human intelligence activities at each level of command.

Acquisition System Protection Program

The protection of all program information throughout the research, development, test, evaluation, and fielding of critical defense technologies and systems.

antiterrorism

Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces. Also called **AT**.

Army G-2X

The Department of the Army executive agent for all Army counterintelligence and human intelligence matters. The Army G-2X serves as the counterintelligence and human intelligence advisor to the Department of the Army G-2. Also called **AG-2X**.

Army theater counterintelligence coordinating authority

The senior counterintelligence element in a theater Army service component command responsible for the technical control and oversight of all counterintelligence activities within their operational purview. Also called **ATCICA**.

communications security

Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Also called **COMSEC**.

contact report

A report used during the conduct of source operations to document the circumstances of, and establish a historical report of the operation.

counterespionage

The aspect of counterintelligence designed to detect, destroy, neutralize, exploit, or prevent espionage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting espionage. Also called **CE**.

counterintelligence

Counters or neutralizes intelligence collection efforts through collection, counterintelligence investigations, operations analysis, production, and technical services and support. Counterintelligence includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies; is the key intelligence community contributor to protect U.S. interests and equities; assists in identifying essential elements of friendly information, identifying vulnerabilities to threat collection, and actions taken to counter collection and operations against U.S. forces. Also called **CI**. (FM 2-0)

counterintelligence coordinating authority

Subordinate to the S/G/J/CX, it provides technical control and oversight for all counterintelligence activities within their area of intelligence responsibility. It provides technical support to all counterintelligence assets and coordinates and deconflicts counterintelligence activities in the deployed area of operations. Also called **CICA**.

counterintelligence force protection source operations

A category of the Army Counterintelligence Collection Program that uses sources to obtain information to answer the commander's information requirements and support protection requirements concerning adversarial, foreign intelligence service, and terrorist collection on U.S. forces and threat indications and warning. Also called **CFSO**.

counterintelligence scope polygraph examination

A polygraph examination using questions reasonably calculated to obtain counterintelligence information, including disclosure of classified information, deliberate damage to or malicious misuse of a United States questions relating to espionage, sabotage, terrorism, unauthorized Government information or defense system, and unauthorized contact with foreign nationals. Also called **CSPE**.

counterintelligence staff officer

A combatant command staff member who serves as the principal counterintelligence advisor to the combatant commander and staff. Also called **CISO**.

counterterrorism

Operations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism. Also called **CT**.

Critical Infrastructure Protection

Focuses on the protection of infrastructures that the Department of Defense designates as critical to mission success. To leverage counterintelligence equities Army counterintelligence employs the functions of investigations, operations, collection, analysis, and production where there is a cyberspace, information systems, or digital media component threat.

cyber counterintelligence activity

Conducts investigations of network intrusion into Army information systems; they support counterintelligence surveys by providing technical advice and assistance to the command concerning computer security posture. Also called **CCA**.

Freedom of Information Act

Enacted in 1966, The Freedom of Information Act (FOIA) is a federal law that establishes the public's right to obtain information from Federal Government agencies. The FOIA is codified at 5 USC § 552. "Any person" can file an FOIA request, including U.S. citizens, foreign nationals, organizations, associations, and universities.

human intelligence

The collection by a trained human intelligence collector of foreign information from people and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment, and capabilities. Also called **HUMINT**. (FM 2-0)

human intelligence operations cell

Assigned under the J/G-2X to track all human intelligence activities in the area of intelligence responsibility. It provides technical support to all human intelligence collection operations and deconflicts human intelligence collection operations in the area of operations. Also called **HOC**.

information assurance

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA. See also information, information tasks, information system.

investigative plan

A document used to plan proposed investigative activities, including special investigative techniques, to support counterintelligence investigation. Also called **IP**.

National Security Threat List

Includes national security threat issues regardless of the country of origin; it includes a classified list of foreign powers that pose a strategic intelligence threat to U.S. security interests.

Office of the National Counterintelligence Executive

The U.S. Government executive agency charged with establishing the strategy for all U.S. counterintelligence agencies to detect, identify, neutralize, and exploit adversarial intelligence. Also called **ONCIX**.

operational control

The authority of command that involves organizing and employing forces, assigning tasks, and designating objectives. Operational control may be exercised at any echelon below the combatant command level. Also called **OPCON**.

operation plan

Any plan for the conduct of military operations in a hostile environment prepared by the commander of a unified or specified command in response to a requirement established by the Joint Chiefs of Staff. Also called **OPLAN**.

operations support cell

An element within the C/J/G/S-2X Section that manages overall 2X Section operations, performs office administration functions, and accomplishes tasks that support both the counterintelligence coordinating authority and the human intelligence operations cell. Also called **OSC**.

This page intentionally left blank.

References

REQUIRED PUBLICATIONS

These documents must be available to the intended user of this publication.

JOINT PUBLICATIONS

JP 2-0. *Joint Intelligence.* 22 June 2007.

JP 2-01. *Joint and National Intelligence Support to Military Operations.* 7 October 2004.

ARMY PUBLICATIONS

AR 15-6. *Procedures for Investigating Officers and Boards of Office*. 2 October 2006.

AR 25-2. *Information Assurance.* 25 October 2007.

AR 27-10. *Military Justice.* 16 November 2005.

AR 190-6. *Obtaining Information from Financial Institutions*. 9 February 2006.

AR 195-6. *Department of the Army Polygraph Activities.* 29 September 1995.

AR 380-10. *Foreign Disclosure and Contacts with Foreign Representative.* 22 June 2007.

AR 380-67. *Personnel Security Program.* 9 September 1988.

AR 380-381. *Special Access Programs (SAPs) and Sensitive Activities.* 21 April 2004.

AR 381-10. *U.S. Army Intelligence Activities.* 3 May 2007.

AR 381-12. *Subversion and Espionage Directed Against the Army (SAEDA).* 15 January 1993.

AR 381-20. *U.S. Army Counterintelligence Activities.* 15 November 1993.

AR 381-45. *Investigative Records Repository.* 25 August 1989.

AR 381-47 (S). *U.S. Army Offensive Counterintelligence Operations (OFCO) (U).* 17 March 2006.

AR 525-13. *Antiterrorism*. 4 January 2002.

AR 530-1. *Operations Security (OPSEC)*. 19 April 2007.

AR 600-8. *Military Personnel Management*. 1 October 1989.

AR 611.201. *Enlisted Career Management Fields and Occupational Specialties*. 26 June 1995.

AR 614-200. *Enlisted Assignments and Utilization Management*. 26 February 2009.

DA Pam 351-4. *U.S. Army Formal Schools Catalog.* 14 January 2006.

DA Pam 600-8. *Management and Administrative Procedures.* 1 August 1986.

FM 2-0. *Intelligence.* 17 May 2004.

FM 2-22.3. *Human Intelligence Collector Operations.* 6 September 2006.

FM 2-22.401. *Multi-Service Tactics, Techniques, and Procedures for Technical Intelligence Operations.* 6 September 2006.

FM 3-0. *Operations.* 27 February 2008.

FM 3-19.13. *Law Enforcement Investigations.* 10 January 2005.

FM 3-19.30. *Physical Security.* 8 January 2007.

FM 34-3. *Intelligence Analysis.* 15 March 1990.

FM 3-24. *Counterinsurgency.* 15 December 2006.

FM 27-10. *Law of Land Warfare.* 18 July 1956.

FM 34-10. *Division Intelligence and Electronic Warfare Operations.* 25 November 1986.

FM 34-8-2. *Intelligence Officers Handbook.* 1 May 1998.

FM 34-37. *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations.* 15 January 1991.

FM 100-15, *Corps Operations.* 29 October 1996.

MCM 2008. *Manual for Courts-Marshal United States*. 21 February 2008.

TC 2-22.303. *The 2X Handbook.* 31 Jul 2006.

TC 2-33.4. *Intelligence Analysis.* 1 July 2009.

OTHER PUBLICATIONS

DODD 5210.48. *Polygraph and Credibility Assessment Program.* 25 January 2007.

DODI 5240.5. *DOD Technical Surveillance Countermeasures (TSCM) Survey Program.* 23 May 1984.

RELATED PUBLICATIONS

These sources contain relevant supplemental information.

ARMY PUBLICATIONS

AR 715-9. *Contractors Accompanying the Force*. 29 October 1999.

FM 3-100.21. *Contractors on the Battlefield*. January 2003.

FMI 4-93.41. *Army Field Support Brigade Tactics, Techniques, and Procedures*. 22 February 2007.

OTHER PUBLICATIONS

DA Pam 715-16. *Contractor Deployment Guide*. 27 February 1998.

AMC Pam 715-18. *AMC Contracts and Contractors Supporting Military Operations*. June 2000.

DCID 1/20. *Security Policy Concerning Travel and Assignment of Personnel with Access to Sensitive Compartmented Information (SCI).* 29 December 1991.

USC Title 10. *Armed Forces*.

USC Title 18. *Crimes and Criminal Procedure.*

REFERENCED FORMS

DA Form 2-1. *Personnel Qualification Record.*

DA Form 1594. *Daily Staff Journal or Duty Officer's Log.*

DA Form 2028. *Recommended Changes to Publications and Blank Forms.*

DA Form 2802. *Polygraph Examination Report.*

DA Form 2823. *Sworn Statement.*

DA Form 3363. *U.S. Army Intelligence Credential (Special Agent).*

DA Form 3363A. *U.S. Army Intelligence Credential (Representative).*

DA Form 3363-1. *U.S. Army Intelligence Credential (Photograph/Signature).*

DA Form 3881. *Rights Warning Procedure/Waiver Certificate.*

DA Form 4137. *Evidence/Property Custody Document.*

DA Form 4187. *Personnel Action.*

DD Form 1610. *Request and Authorization for TDY Travel of DOD Personnel.*

FD-258. *FBI Fingerprint Card.*

SF 86. *Questionnaire for National Security Positions.*

SF 702. *Security Container Checksheet.*

Index

A

analysis and production, 1-3, 1-4, 1-16, 3-1, 3-4, 3-8, 5-3, 7-4, F-6, G-3

antiterriorism, 3-4

B

badge and credentials, 1-8, 2-1, 2-5, 2-9, 2-23, 2-33, 2-43, A-6, A-7, A-8, A-10, J-1

BIGOT cases, 2-19

biometrics, 6-7, 6-8

C

civil operations, 3-6

collection, 1-1, 1-3, 1-4, 1-11, 1-12, 1-14, 1-15, 1-16, 1-17, 3-1, 3-4, 4-1, 4-2, 4-3, 4-10, 4-11, 4-12, 5-2, 5-3, 5-8, 7-3, 8-8, B-1, C-1, E-49, F-5, G-3, H-3, H-7

computer forensics, 1-12, 1-14, 6-1, 6-8, 7-1, 7-2, 7-10, H-8

contractor support, B-1, F-7

core competencies, 1-3, 1-4

counterdrug operations, 3-7

Counterintelligence Awareness and Reporting Program, 2-12

counterintelligence awareness briefing, 1-16, 1-17, 2-41, 3-5

counterintelligence coordinating activity (CICA), 1-4, 1-5, 1-6, 1-7, 1-9, 1-10, 1-15, 1-16, 2-6, 2-14, 2-16, 4-3, 5-2, 5-5, 5-8, 9-3, 9-5, F-5, F-6, G-2, H-5

counterintelligence force protection source operations (CFSO), 1-8, 3-1, 4-2, 4-6, F-4

counterintelligence incident report, 2-7, 2-8, 2-9, 2-21, 2-41, 2-46, 3-1, 8-2, 8-12, 8-25

counterintelligence investigations, F-6

counterintelligence materials, 3-2

counterintelligence operational management team (OMT), 1-4, 1-10, 1-12, 1-18, 5-2, 9-3, 9-4, 9-5, H-3, H-5, H-6, H-7

counterintelligence team, 1-4, 1-10, 1-11, 1-12, 1-18, 5-8, 5-21, 7-4, 9-3, 9-4, 9-5, C-4, F-1, F-2, F-3, F-4, G-3, H-2, H-5, H-6, H-7, H-8

covering agent program, 3-2, 4-5, F-2

cyber counterintelligence operations, 7-3

D

debriefing, 1-3, 1-11, 1-12, 2-3, 2-10, 2-35, 3-5, 3-9, 3-10, 3-11, 3-12, 4-2, 4-3, 4-4, 4-5, 7-4, B-2, C-6, C-7, C-8

defensive source operations (DSO), 3-1, 4-2, 4-6

document and media exploitation (DOMEX), 1-9, 7-4, H-8, H-9

E

electronic surveillance, 6-1, 8-7

evidence, 1-2, 2-2, 2-3, 2-8, 2-15, 2-18, 2-19, 2-20, 2-22, 2-48, 3-14, 4-3, 5-2, 6-1, 6-2, 6-3, 6-8, 7-1, 7-2, 7-9, 7-10, 7-12, 7-13, 7-14, 8-4, 8-5, 8-6, 8-7, 8-12, 8-13, 8-14, 8-15, E-57, I-4

F

Federal Bureau of Investigation (FBI), 1-13, 2-4, 2-23, 2-26, 2-45, 2-46, 2-47, 4-9, 8-3, 8-12, A-3, D-1, E-50, H-2, I-6

foreign intelligence and security services (FISS) and international terrorist organizations (ITO), F-4

foreign intelligence services (FISS), vii, 1-1, 1-3, 1-4, 1-11, 1-14, 2-4, 3-1, 3-6, 4-1, 5-2, 6-5, 7-1, A-1

H

Homeland Defense, 3-6

human intelligence (HUMINT), 1-1, 1-2, 1-3, 1-6, 1-9, 1-12, 1-14, 4-1, 4-6, 4-7, 7-4, H-5

I

information superiority, 1-5, 3-7, 3-8, 3-11, 6-5, 6-9

intelligence preparation of the battlefield (IPB), 5-3, 5-5, 5-20, 5-21, F-1

international terrorist organizations (ITO), vii, 1-1, 1-3, 1-4, 1-11, 1-14, 2-4, 3-1, 3-6, 4-1, 5-2, 6-5, 7-1, A-1

interpreter support, C-3

investigations, vii, 1-1, 1-3, 1-4, 1-8, 1-11, 1-12, 1-13, 1-14, 1-15, 1-16, 1-17, 1-18, 2-1, 2-2, 2-6, 2-7, 2-10, 2-11, 2-14, 2-18, 2-20, 2-21, 5-2, 5-8, 5-15, 6-1, 6-2, 6-3, 6-5, 6-6, 6-8, 7-1, 7-2, 7-3, 7-4, 7-6, 8-2, 8-3, 8-4, 9-3, C-1, C-3, D-2, E-45, I-2

J

Joint Interrogation and Debriefing Center (JIDC), 4-6, 4-7

Joint Terrorism Task Force (JTTF), 2-24, 2-27, 3-7

jurisdiction, 1-12, 1-13, 2-2, 2-3, 2-4, 2-5, 2-6, 2-10, 2-12, 2-17, 2-38, 2-39, 2-41, 2-43, 2-47, 4-8, 4-9, 7-2, 7-3, 8-2, 8-3, 8-4, 8-6, 8-9, 8-10, 8-13, 8-15, 8-16, 8-23, 8-25, D-1

L

legal principles, 2-18, 8-1, 8-2, I-2

levels of employment, 1-14

liaison, 1-3, 1-8, 1-9, 1-11, 1-12, 1-16, 1-18, 2-8, 2-19, 2-23, 2-27, 3-2, 3-5, 3-6, 3-7, 3-13, 4-2, 4-3, 4-8, 4-9, 4-10, 7-4, C-1, C-7, F-2, G-2, G-3

M

multinational operations, 1-16, G-1, G-2

O

Offensive Counterintelligence Operations (OFCO), 1-14, 4-2

operations, vii, 1-1, 1-2, 1-3, 1-4, 3-1
operations security (OPSEC), 2-6, 2-7, 2-18, 2-19, 2-21, 3-6, 3-7, 3-10, 4-11, 5-5, C-5, F-3, G-3
oversight, 1-8, 1-10, 1-13, 1-14, 1-15, 1-16, 1-18, 2-6, 2-14, 2-18, 2-22, 2-34, 2-45, 8-1, 8-6, 9-1, 9-2, F-2, F-6, F-7

P

physical surveillance, 2-17, 6-2
planning, vii, 1-6, 1-11, 1-14, 2-2, 2-11, 2-14, 2-15, 2-18, 2-46, 3-1, 3-5, 3-11, 4-2, 4-6, 4-11, 5-2, 5-5, 5-21, C-4, F-1, F-2, G-1, G-2, H-9
polygraph, 1-4, 1-8, 1-11, 1-12, 2-16, 2-25, 2-45, 6-1, 6-2, 6-3, 6-4, C-4, C-8
probationary program, A-6, A-11
protection, 1-3, 1-4, 1-5, 1-12, 1-16, 1-17, 3-1, 3-5, 3-6, 3-7, 4-2, 4-6, 4-12, 5-2, 5-5, 6-7, 6-8, 9-4, 9-5, F-3, G-1, G-2

R

red team, 3-3, 3-4, 7-3
report writing, 9-1, E-1
research and technology protection (RTP), 1-4, 1-5, 1-14, 3-2, 3-4

S

screening, 1-2, 1-3, 1-8, 1-11, 1-12, 1-16, 1-17, 2-1, 3-5, 3-9, 3-10, 3-11, 3-12, 4-2, 4-3, 4-5, 4-6, 4-7, 6-8, 7-4, F-4
search and seizure, 3-14, 6-8, 7-9, 7-10, 8-12, 8-15
standing counterintelligence collection requirements, 1-3, 2-12, 4-5, 4-12

T

technical counterintelligence services, 1-14, 6-1, 7-4
technical surveillance countermeasures (TSCM), 1-4, 1-8, 1-12, 6-5, 6-6, 6-7

V

vulnerability assessment, 1-8, 1-14, 1-16, 1-17, 2-1, 3-2, 3-5, 3-6, 3-10, 4-12, 4-13, 5-4, 5-5, 6-9, 7-3, 7-4

FM 2-22.2
21 October 2009

By order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
0927305

DISTRIBUTION:

Active Army, the Army National Guard, and the United States Army Reserve: Not to be distributed; electronic media only.