

Army Regulation 381-20

Military Intelligence

The Army Counterintelligence Program

Distribution Restriction Statement.
This regulation contains operational information for official Government use only. Distribution is limited to U.S. Government agencies. Requests from outside the U.S. Government for release of this regulation under the Freedom of Information Act or Foreign Military Sales Program must be made to HQDA (DAMI-CIC), Washington, DC 20310-1054.

Destruction Notice.
Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Headquarters
Department of the Army
Washington, DC
15 November 1993

UNCLASSIFIED

SUMMARY of CHANGE

AR 381-20

The Army Counterintelligence Program

This revision--

- o Expands investigative responsibilities to all Army counterintelligence units (CI), and specifies investigative jurisdictions (chap 2).
- o Establishes the CI control office system (chap 3).
- o Clarifies collection authority (chap 6).
- o Requires CI analysis and production at all levels with staff capability (chap 7).
- o Permanently issues badges and credentials to CI personnel serving in designated assignments (para 9-4).
- o Provides authority for conducting intelligence polygraphs (para 10-2).

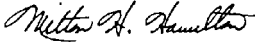
Military Intelligence

The Army Counterintelligence Program

By Order of the Secretary of the Army:

GORDON R. SULLIVAN
General, United States Army
Chief of Staff

Official:


MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army

History. This UPDATE printing publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation implements Department of Defense (DOD) Directives 4640.6, 5210.48, 5210.48-R, 5210.84, 5240.2, 5240.4, 5240.8, 5240.10; DOD memorandum of 28 December 1989, subject: Counterintelligence Collection and Production Policy; the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, 5 April, 1979; and the Attorney General Guidelines for FBI Supervision or Conduct of Espionage Investigations of U. S. Diplomatic Missions Personnel Abroad, 17 April, 1990. It establishes authority and responsibility for the Army Counterintelligence Program, and includes guidance on the conduct of and jurisdiction over counterintelligence investigations, operations, collection, analysis, and production.

Applicability. This regulation applies to the Active Army, the Army National Guard, and the U.S. Army Reserve. This

regulation also applies to all Army intelligence components, other military personnel and civilian personnel of the Department of the Army when they engage in counterintelligence activities, and members of the U.S. Army Reserve and the Army National Guard when they perform Federal counterintelligence duties. During mobilization or national emergency this regulation remains in effect without change.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Intelligence (DCSINT). Subject to the reservations set out below, the DCSINT has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The DCSINT may delegate this approval authority, in writing, to a division chief under their supervision within the proponent agency in the grade of colonel or the civilian equivalent.

Recordkeeping Requirements
This regulation requires the creation, maintenance, and use of the following specific records. (See app B of AR 25-400-2 for file numbers (FNs), descriptions, and dispositions.)
FN 380-13b, *Non-DOD affiliated personnel and organizations*
FN 380-13c, *Counterintelligence special operations*
FN 381-20b, *Captured information*
FN 381-20c, *Credentials and badge controls*
FN 381-20d, *Counterintelligence collection files*
FN 381-20e, *Counterintelligence production files*
FN 381-20f, *Counterintelligence information request*
FN 381-20g, *Counterintelligence spot reports*
FN 381-20i, *Foreign personnel and organizations*

FN 381-20l, *Counterintelligence surveys and inspections*
FN 381-20m, *Local intelligence, counterintelligence, and security files*
FN 381-45c, *DOD-affiliated personnel and incident investigations*
FN 381-45d, *Intelligence/counterintelligence source*

Army management control process. Following a review of guidance in AR 11-2, it is determined that this regulation does not contain management control provisions.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from HQDA (DAMI-CIC), WASH DC 20310-1054.

Interim changes. Interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI-CIC), Washington, DC 20310-1054.

Distribution. Distribution of this publication is made in accordance with the requirements on DA Form 12-09-E, block number 2410, intended for command levels A,B,C,D, and E for the Active Army, the Army National Guard, and the U.S. Army Reserve.

Distribution Restriction Statement.

This regulation contains operational information for official Government use only. Distribution is limited to U.S. Government agencies. Requests from outside the U.S. Government for release of this regulation under the Freedom of Information Act or Foreign Military Sales Program must be made to HQDA (DAMI-CIC), Washington, DC 20310-1054.

Destruction Notice.

Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

*This change supersedes AR 381-20, 17 April 1987, and rescinds DA Form 4354-R, 1 August 1975.

Contents (Listed by paragraph and page number)

Chapter 1

General, page 1

Purpose • 1-1, *page 1*

References • 1-2, *page 1*

Explanation of abbreviations and terms • 1-3, *page 1*

Authority • 1-4, *page 1*

Mission and policy • 1-5, *page 1*

Chapter 2

Responsibilities, page 2

Army General Counsel (AGC) • 2-1, *page 2*

The Inspector General (TIG) • 2-2, *page 2*

The Judge Advocate General (TJAG) • 2-3, *page 2*

Deputy Chief of Staff for Intelligence (DCSINT) • 2-4, *page 2*

The Deputy Chief of Staff for Personnel (DCSPER); the Commanding General, U.S. Army Personnel Command (CG, PERSCOM); and the Commanding General, U.S. Army Reserve Personnel Center (CG, ARPERCEN) • 2-5, *page 2*

Commanding General, U.S. Army Training and Doctrine Command (CG, TRADOC) • 2-6, *page 2*

Commanding General, U.S. Army Materiel Command (CG, AMC) • 2-7, *page 3*

Commander in Chief, U.S. Army, Europe (CINCUSAREUR); Commanding General, U.S. Army Forces Command (CG, FORSCOM); Commanding General, Eighth U.S. Army (CG, EUSA); Commanding General, U.S. Army Pacific Command (CG, USARPAC); and Commanding General, U.S. Army South (CG, USARSO) • 2-8, *page 3*

Commanding General, Third U.S. Army (CG, TUSA) • 2-9, *page 3*

Commanding General, U.S. Army Special Operations Command (CG, USASOC) • 2-10, *page 3*

Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM) • 2-11, *page 4*

Commander, 650th MI Group • 2-12, *page 5*

Commanding General, U.S. Army Criminal Investigation Command (CG, USACIDC) and Commander, U.S. Army Military Police Operations Agency (Cdr, USAMPOA) • 2-13, *page 5*

Commanders of all major Army commands (MACOMs), major subordinate commands, chiefs/executives of HQDA and field operating agencies/activities • 2-14, *page 5*

Chief, U.S. Army Reserve; Commander, U.S. Army Reserve Command; and Chief, National Guard Bureau • 2-15, *page 5*

U.S. Army Intelligence and Threat Analysis Center (USAITAC) • 2-16, *page 5*

All commanders with assigned or attached CI personnel • 2-17, *page 5*

Chapter 3

Control Offices, page 6

General • 3-1, *page 6*

Army Central Control Office • 3-2, *page 6*

Sub-control offices • 3-3, *page 6*

Chapter 4

Counterintelligence Investigations, page 7

General • 4-1, *page 7*

Investigations under Army CI jurisdiction • 4-2, *page 7*

Personnel security investigations • 4-3, *page 8*

Reporting requirements • 4-4, *page 8*

Shared investigative responsibility and joint investigations • 4-5, *page 8*

Jurisdiction over Army personnel at U.S. missions abroad • 4-6, *page 9*

Impersonation of DA military intelligence personnel or the fabrication, unauthorized possession or use of military intelligence documentation • 4-7, *page 9*

Use of the National Crime Information Center (NCIC) • 4-8, *page 9*

Release of investigative information • 4-9, *page 9*

Contents—Continued

Chapter 5

Counterintelligence Operations and Techniques, page 10

Section I

Counterintelligence Special Operations, page 10

General • 5-1, *page 10*

Operations • 5-2, *page 10*

Section II

Counterintelligence General Operations, page 10

General • 5-3, *page 10*

CI support to force protection • 5-4, *page 10*

Low level source operations (LLSO) • 5-5, *page 10*

Advice and assistance • 5-6, *page 10*

Counterintelligence technical support activities • 5-7, *page 11*

CI support to acquisition and special access programs • 5-8, *page 11*

CI support to HUMINT • 5-9, *page 11*

CI support to treaty verification • 5-10, *page 11*

Liaison • 5-11, *page 11*

CI support to domestic civil disturbances • 5-12, *page 12*

CI support to natural disaster operations • 5-13, *page 12*

Section III

Counter-Signals Intelligence (C-SIGINT), page 12

General • 5-14, *page 12*

Counter-SIGINT support • 5-15, *page 12*

Section IV

Techniques, page 13

General • 5-16, *page 13*

Vulnerability assessments • 5-17, *page 13*

Hostile intelligence simulation (Red Team) • 5-18, *page 13*

Covering agent support • 5-19, *page 13*

Chapter 6

Counterintelligence Collection, page 13

General • 6-1, *page 13*

Identifying and validating collection requirements • 6-2, *page 14*

Collection and reporting procedures • 6-3, *page 14*

Local operational data • 6-4, *page 14*

Debriefings and interrogations • 6-5, *page 14*

Returned U.S. defector debriefings • 6-6, *page 14*

Chapter 7

Counterintelligence Analysis and Production, page 15

General • 7-1, *page 15*

Analysis • 7-2, *page 15*

Production • 7-3, *page 16*

Chapter 8

Employment, Use, and Special Administration of U.S. Army Counterintelligence Personnel and Authority of CI Special Agents, page 16

Section I

Employment, Use, and Special Administration of U.S. Army Counterintelligence Personnel, page 16

Personnel involvement • 8-1, *page 16*

Contents—Continued

Assignment of CI personnel • 8-2, *page 16*
Duty limitations • 8-3, *page 16*
Withdrawal of SSI/MOS/civilian specialty • 8-4, *page 17*
Clothing and grade • 8-5, *page 17*
Nonstandard spectacles • 8-6, *page 18*
Access to military privileges • 8-7, *page 18*
Billets, mess, and temporary duty • 8-8, *page 18*
Weapons • 8-9, *page 18*

Section II

Authority of CI Special Agents, page 18
Freedom of movement • 8-10, *page 18*
Oath administration • 8-11, *page 18*
Apprehension authority • 8-12, *page 18*
Search and seizure authority • 8-13, *page 19*
Involvement in civil legal proceedings • 8-14, *page 19*
Access to records, information, and facilities • 8-15, *page 19*
CI special agents assigned to Special Mission Units • 8-16, *page 19*

Chapter 9

The U.S. Army Intelligence Badge and Credential Program, page 19

General • 9-1, *page 19*
Program functions • 9-2, *page 20*
Issue and retention of badges and credentials • 9-3, *page 20*
Criteria for issue of representative credentials • 9-4, *page 20*
Initial B&C issue by other than USAIC • 9-5, *page 21*
Loss of B&C and representative credentials • 9-6, *page 21*
Misuse of B&C and representative credentials • 9-7, *page 21*
Central badge and credentials repository • 9-8, *page 22*
The Counterintelligence Badge Trophy Program • 9-9, *page 22*

Chapter 10

Intelligence Polygraphs, page 22

General • 10-1, *page 22*
Use of intelligence polygraph examinations • 10-2, *page 22*
Selection, training, and certification of intelligence polygraphers • 10-3, *page 23*
Requesting intelligence polygraph support • 10-4, *page 23*

Appendixes

- A.** References, *page 24*
- B.** Security Considerations, *page 30*
- C.** Selected Counterintelligence Addresses, *page 31*
- D.** Courtesy Letter Program, *page 33*
- E.** Counterintelligence Scope Polygraph Program, *page 35*

Glossary

Index

Chapter 1 General

1-1. Purpose

This regulation sets forth the policy, responsibilities, jurisdictions and procedures for the Army Counterintelligence (CI) Program.

1-2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Authority

Army CI authority is derived from the following:

- a. Executive Order 12333, United States Intelligence Activities.
- b. 18 USC 801-940, The Uniform Code of Military Justice (UCMJ).
- c. Section 1801, title 50, United States Code (50 USC 401), The National Security Act of 1947.
- d. Section 401, title 50, United States Code (50 USC 1801), The Foreign Intelligence Surveillance Act of 1978.
- e. Public Law 100-180, Defense Authorization Act for Fiscal Years 1988 and 1989.
- f. Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation (FBI), 5 April, 1979.
- g. Attorney General Guidelines for FBI Supervision or Conduct of Espionage Investigations of U.S. Diplomatic Missions Personnel Abroad, 17 April, 1990.
- h. Department of Defense (DOD) Directive 4640.6, Communications Security Monitoring.
- i. DOD Directive 5210.48, DOD Polygraph Program.
- j. DOD Directive 5240.2, DOD Counterintelligence.
- k. DOD Instruction 5240.10, DOD Counterintelligence Support to Unified and Specified Commands.
- l. DOD memorandum of 28 December 1989, subject: Counterintelligence Collection and Production Policy.

1-5. Mission and policy

a. *Mission.* The Army will conduct aggressive, comprehensive, and coordinated counterintelligence activities worldwide, to detect, identify, assess, and counter, neutralize, or exploit the intelligence collection efforts, other intelligence activities, sabotage, subversion, sedition, terrorist activities, and assassination efforts of foreign powers, organizations, or persons directed against Department of the Army (DA) or DOD personnel, information, materiel, and activities. This mission will be accomplished during peacetime and all levels of conflict.

b. *Policy.*

(1) The Army will maintain a CI program and a professional CI force, which will be trained and equipped to carry out its mission of opposing foreign intelligence and security services (FIS) activities. FIS activities include both those identifiable as intelligence collection (Human Intelligence [HUMINT], Signals Intelligence [SIGINT], Imagery Intelligence [IMINT]) and FIS activities that have other objectives (analysis and production, assassination, counterintelligence, deception, disinformation, propaganda, sabotage, sedition, subversion).

(2) Army CI elements will execute the CI mission in concert and coordination with other DOD and non-DOD members of the foreign counterintelligence community to ensure overall effectiveness of the national CI effort.

(3) Counterintelligence, under the authority cited in paragraphs 1-4a, 1-4j and 1-4k, excludes the management and execution of security countermeasures for personnel, physical, document or communications security programs; operations security; or counterimagery.

(4) The Army CI Program will be conducted pursuant to executive orders, statutes, DOD directives, Army regulations and guidance, and interagency agreements governing CI activities.

(5) Refer all questions of legal interpretation and intelligence oversight to the supporting staff judge advocate office. Forward questions involving operational interpretation of this regulation to Headquarters, Department of the Army (HQDA) (DAMI-CIC). Forward, through command channels, to HQDA (DAMI-IO), Washington, DC 20310-1001, requests for interpretation of policy concerning intelligence oversight (AR 381-10) which cannot be resolved locally.

(6) This regulation is the basis for all Army CI policy. If conflicts are discovered between this regulation and other Army CI regulations, this document takes precedence.

Chapter 2 Responsibilities

2-1. Army General Counsel (AGC)

The AGC is the legal counsel to the Secretary of the Army and the chief legal officer of the Department of the Army. The AGC's responsibility extends to any subject of law and other matters as directed by the Secretary. The AGC will—

- a.* Exercise the Secretary's oversight of intelligence activities, and monitor sensitive Army intelligence, criminal investigative, and special activities for legality and propriety.
- b.* Review issues relating to intelligence activities prior to a decision by any Secretariat official.
- c.* Conduct all formal Army coordination with Department of Justice senior officials on intelligence matters.

2-2. The Inspector General (TIG)

TIG will exercise oversight of intelligence activities as prescribed by AR 381-10, prepare the DA Quarterly Intelligence Oversight Activities Report, and maintain liaison with the Assistant to the Secretary of Defense (Intelligence Oversight) concerning DOD intelligence matters.

2-3. The Judge Advocate General (TJAG)

By statute, TJAG is the legal advisor to the Secretary and all officers and agencies of the Department of the Army. TJAG will provide legal advice directly to the Chief of Staff of the Army (CSA) and members of the Army Staff; and legal advice to the Secretary and other officials of the Office of the Secretary of the Army in coordination with the AGC.

2-4. Deputy Chief of Staff for Intelligence (DCSINT)

The DCSINT will—

- a.* As the Army senior official of the intelligence community, exercise Army staff responsibility for the Army CI Program, as directed by the Secretary of the Army and the CSA, under provisions of (UP) AR 10-5.
- b.* Implement DOD and higher CI policy, develop Army policy and procedures, and provide interpretation as required.
- c.* Exercise Army staff responsibility for CI training.
- d.* Represent DA to DOD and other Federal departments and agencies concerned with CI policy, activities, issues of major significance, and oversight of intelligence programs.
- e.* Provide information and reports as required to DOD and other departments and agencies concerned with CI activities and the Intelligence Oversight Program.
- f.* Coordinate DA or higher level approvals of CI activities when required.
- g.* Ensure that Army CI activities comply with established guidelines and restrictions and that all matters specified by AR 381-10 are referred, as appropriate, to the Army leadership.
- h.* Exercise general staff supervision over and establish policies regarding the procurement, manufacture, issue, use, control, and disposition of U.S. Army Intelligence (USAI) badges and credentials, representative credentials, and associated items.

2-5. The Deputy Chief of Staff for Personnel (DCSPER); the Commanding General, U.S. Army Personnel Command (CG, PERSCOM); and the Commanding General, U.S. Army Reserve Personnel Center (CG, ARPERCEN)

These commanders will—

- a.* Administer and supervise the personnel management aspects of the Army CI Program, in accordance with DOD 5210.48, DOD 5240.5, AR 195-6, AR 381-14(S), this regulation, and applicable personnel policy, including a probationary program for newly trained CI officers, agents, assistants, and civilians.
- b.* Evaluate 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 program.
- c.* Provide the DCSINT, DA with statistical data as required for the development of CI policy and programs.

2-6. Commanding General, U.S. Army Training and Doctrine Command (CG, TRADOC)

The CG, TRADOC will—

- a.* Develop doctrinal literature and training programs for the Army CI Program.
- b.* Conduct formal CI training for officers, warrant officers, and enlisted personnel accepted into the CI program. Train civilian CI personnel in established military CI courses.
- c.* Ensure the quality, timeliness, and relevance of formal CI training programs.

d. Serve as combat developer for CI collection and analysis systems, specialized intelligence materiel to support CI investigations and operations, and COMSEC monitoring equipment.

2-7. Commanding General, U.S. Army Materiel Command (CG, AMC)

The CG, AMC will—

a. Provide materiel and related logistics services for CI collection and analysis systems, specialized intelligence materiel, and COMSEC monitoring equipment.

b. Coordinate with CG, INSCOM in establishing Counter-SIGINT support to friendly communications-electronics (C-E) systems during the Research, Development, Test, and Evaluation (RDTE) process.

2-8. Commander in Chief, U.S. Army, Europe (CINCUSAREUR); Commanding General, U.S. Army Forces Command (CG, FORSCOM); Commanding General, Eighth U.S. Army (CG, EUSA); Commanding General, U.S. Army Pacific Command (CG, USARPAC); and Commanding General, U.S. Army South (CG, USARSO)

These commanders will—

a. Conduct CI operations and investigations in their respective areas of responsibility (AOR), in coordination with the technical control of the appropriate sub-control office, pursuant to the policy set forth in this regulation and applicable memoranda of understanding (MOU).

b. Collect and report CI information in response to approved intelligence collection requirements and general HUMINT tasking for which CI elements have a capability.

c. Perform CI analysis and production to satisfy needs within the AOR.

d. Conduct CI-related liaison with host and other foreign country agencies and representatives of other U.S. agencies as outlined in chapter 5.

e. Ensure the Unified Command is kept fully apprised of and expeditiously informed of Army CI activities that could jeopardize life, involve foreign policy, embarrass the U.S. Government, or have other significant consequences. At the minimum, provide a semiannual briefing on investigations, offensive CI operations, collection activities, and production that are relevant to the command or occur within the command's area of responsibility.

f. In coordination with the theater sub-control office, immediately pass to the U.S. Army Criminal Investigation Command (USACIDC) any information developed in the course of CI activities that is subject to USACIDC criminal investigative jurisdiction per AR 195-2.

g. Provide immediately to the installation provost marshal, nearest USACIDC office, and all affected activities, information on terrorism and other threats to physical safety developed during the course of CI activities; and report this information to the U.S. Army Intelligence and Threat Analysis Center (USAITAC) and the U.S. Army Antiterrorism Operations and Intelligence Cell (ATOIC).

h. In overseas AOR, conduct personnel security investigations (PSI) in coordination with the Defense Investigative Service (DIS) and the U.S. Army Intelligence and Security Command.

2-9. Commanding General, Third U.S. Army (CG, TUSA)

The CG, TUSA will—

a. Perform CI analysis and production to satisfy needs prior to and upon deployment of forces.

b. Collect and report CI information in response to approved intelligence collection requirements and general HUMINT tasking for which CI elements have the capability.

c. Ensure the unified command is kept fully and expeditiously informed of Army CI activities that could jeopardize life, involve foreign policy, embarrass the U.S. Government, or have other significant consequences. At the minimum, provide a semiannual briefing on investigations, offensive CI operations, collection activities, and production that are relevant to the command or occur within the command's area of responsibility.

d. In coordination with the theater sub-control office, immediately pass to the USACIDC any information developed in the course of CI activities that is subject to USACIDC criminal investigative jurisdiction.

e. Provide immediately to the installation provost marshal, nearest USACIDC office, and all affected activities, information on terrorism and other threats to physical safety developed during the course of CI activities; and report this information to USAITAC and ATOIC.

f. Upon deployment of forces, conduct CI operations and investigations in accordance with the policy set forth in this regulation.

g. Upon deployment of forces, conduct CI-related liaison with host and other foreign country agencies and representatives of other U.S. agencies as outlined in chapter 5.

h. In overseas AOR, conduct PSI in coordination with DIS and the U.S. Army Intelligence and Security Command.

2-10. Commanding General, U.S. Army Special Operations Command (CG, USASOC)

The CG, USASOC will—

a. Perform CI analysis and production to satisfy command requirements.

- b.* Collect and report CI information in response to approved intelligence collection requirements and general HUMINT tasking for which CI elements have the capability.
- c.* Ensure the Unified Command is kept fully and expeditiously informed of Army CI activities that could jeopardize life, involve foreign policy, embarrass the U.S. Government, or have other significant consequences. At the minimum, provide a semiannual briefing on investigations, collection activities, and production that are relevant to the command or occur within the command's area of responsibility.
- d.* In coordination with the appropriate theater sub-control office, immediately pass to the USACIDC any information developed in the course of CI activities that is subject to USACIDC criminal investigative jurisdiction.
- e.* Provide immediately to the installation provost marshal, nearest USACIDC office, and all affected activities, information on terrorism and other threats to physical safety developed during the course of CI activities; and report this information to USAITAC and ATOIC.
- f.* When elements or units are deployed for training or operations on Joint Chiefs of Staff directive, conduct CI operations and investigations in direct support of the deployment, IAW the policy set forth in this regulation.
- g.* Conduct CI-related liaison with host and other foreign country agencies and representatives of other U.S. agencies as outlined in chapter 5.

2-11. Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM)

The CG, INSCOM will—

- a.* Conduct theater and strategic CI activities in accordance with the policy set forth in this regulation and AR 10-87.
- b.* Establish and operate a central control system for all Army CI controlled activities.
- c.* Establish and operate the Army Central Control Office (ACCO) and sub-control offices (SCO) in coordination with the appropriate theater Army component commander, UP chapter 3. Establish one SCO in each theater with forward-deployed Army forces, except as stated in paragraph 2-12*b*. Upon deployment of Army elements into other areas, establish SCO as required.
- d.* Collect and report CI information in response to approved intelligence collection requirements and general HUMINT tasking for which CI has a capability.
- e.* Ensure that the DCSINT is provided details of significant CI controlled activities so that Army leadership may be informed, especially incidents which meet the criteria in AR 381-12, AR 381-47 (S), or any HQDA supplementing guidance.
- f.* Periodically disseminate products on closed CI cases, in support of the Subversion and Espionage Directed Against the Army (SAEDA) Program (AR 381-12).
- g.* Assist CG, TRADOC in developing concepts, architecture, techniques, tactics, and procedures for conducting Counter-SIGINT vulnerability assessments and COMSEC monitoring activities.
- h.* Assist CG, TRADOC in developing CI collection and analysis systems and specialized intelligence materiel to support CI investigations and operations.
- i.* Manage the intelligence polygraph and TSCM programs, including command and control and certification of intelligence polygraph examiners, certification of TSCM personnel, and the acquisition of intelligence polygraph and TSCM equipment (see AR 195-6 and AR 381-14 (S)).
- j.* Conduct liaison with the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), host and other foreign country agencies, and other federal and local agencies on CI operations and investigations, as outlined in chapter 5.
- k.* Immediately pass to the USACIDC any information developed in the course of CI activities which is subject to USACIDC criminal investigative jurisdiction per AR 195-2.
- l.* Provide immediately to the installation provost marshal, nearest USACIDC office, and all affected activities, information on terrorism and other threats to physical safety developed during the course of CI activities; and report this information to USAITAC and ATOIC.
- m.* Manage the USAI Badge and Credential Program. (See chap 9 for specific program functions.)
- n.* Assist the Navy and Army Military Police in the Port Security Program in accordance with DOD Dir 5100.78, FM 19-30, and applicable MOU.
- o.* Provide CI support to the Defense Mapping Agency and the Defense Nuclear Agency, in fulfillment of the Army's executive agent responsibilities assigned by DOD.
- p.* Provide CI and threat assessment support to selected DOD and DA special access programs (SAP) and Army acquisition programs, and CI support to treaty verification.
- q.* Implement the DA Automated Information Systems Security Assessment Program and the Computer Security Technical Vulnerability Reporting Program.
- r.* Upon request, brief unified commanders on INSCOM CI activities that are relevant to the command or occur within the command's area of responsibility.

s. Manage and conduct overseas PSI, in coordination with DIS and overseas commands, except as stated in paragraph 2-12.

2-12. Commander, 650th MI Group

The Commander, 650th MI Group will—

- a. Under the command and control of the Supreme Allied Command Europe, provide CI support to Allied Command Europe (ACE) in accordance with applicable NATO/ACE policy and this regulation.
- b. As an exception to paragraph 2-11c, establish and operate a CI sub-control office, UP paragraph 3-3.
- c. Conduct liaison with host and other foreign country agencies and representatives of other U.S. and NATO agencies, in compliance with ACE and NATO directives.
- d. Conduct CI analysis and production to support ACE requirements.
- e. Operate and maintain a TSCM program, in compliance with ACE directives and AR 381-14 (S).
- f. Manage and conduct PSI for U.S. personnel assigned to ACE, in coordination with DIS.

2-13. Commanding General, U.S. Army Criminal Investigation Command (CG, USACIDC) and Commander, U.S. Army Military Police Operations Agency (Cdr, USAMPOA)

These commanders will—

- a. Immediately provide to the supporting Army CI component any information developed during the course of criminal investigations that meet the criteria of national security crimes, as described in chapter 4, and information of CI interest as defined in AR 381-12.
- b. Provide support, when requested, to CI investigations.
- c. Provide to the supporting Army CI component the identity of subjects of criminal investigative activity who possess a security clearance.
- d. Report terrorist-related information to the supporting Army CI component, USAITAC and ATOIC.

2-14. Commanders of all major Army commands (MACOMs), major subordinate commands, chiefs/executives of HQDA and field operating agencies/activities

These officials will—

- a. Establish procedures to ensure that information of CI interest, especially known or suspected acts of espionage, is expeditiously reported to the supporting CI component.
- b. Facilitate the conduct of intelligence polygraphs, CI investigative, operational, collection, and analysis and production activities, as they affect the organization.
- c. Conduct such CI analysis and production as is required by the element, within its capability. Provide copies of MACOM CI production to USAITAC.

2-15. Chief, U.S. Army Reserve; Commander, U.S. Army Reserve Command; and Chief, National Guard Bureau

These officials will—

- a. Implement appropriate CI activities upon unit mobilization or call to active Federal service.
- b. Develop annual training and inactive duty training programs for Reserve Components (RC) CI personnel to promote technical proficiency and enhance the development of individual and unit CI skills.

2-16. U.S. Army Intelligence and Threat Analysis Center (USAITAC)

USAITAC will provide strategic counterintelligence analysis and production to satisfy validated intelligence production requirements, under the operational control of DCSINT.

2-17. All commanders with assigned or attached CI personnel

These commanders will—

- a. Ensure that assigned/attached CI personnel are employed in accordance with this regulation.
- b. Ensure that CI personnel meet the standards of performance, conduct, and suitability prescribed in personnel regulations and chapter 8.
- c. Ensure that CI personnel are fully aware of and comply with their individual responsibilities as outlined in AR 381-10.

Chapter 3 Control Offices

3-1. General

a. A network of control offices exercises centralized technical direction, control, coordination, and oversight of Army CI controlled activities. This network is designed to—

- (1) Centralize technical control and decentralize execution.
- (2) Ensure integration and full coordination.
- (3) Provide an objective system of technical review, which ensures complete and proper accounting of activities; compliance with established policies; opening, scoping and closing cases; interagency coordination; analysis of reports; and archiving.

b. All Army CI controlled activities will be conducted or monitored under this control office system.

c. Report conflicts between control offices concerning opening, scoping, conduct, suspension, termination, or closing of cases, to HQDA and INSCOM. HQ, INSCOM will resolve the conflict or forward to HQDA if required.

3-2. Army Central Control Office

The Army Central Control Office (ACCO) exercises technical control, review, coordination and oversight of CI controlled activities. The ACCO will be staffed by personnel experienced in CI controlled activities, especially in investigation. The ACCO will—

a. Provide an objective system of technical review which will ensure complete and proper accounting of CI controlled activities, and compliance with established policy.

b. Open CI investigations and assign all case control numbers; monitor low level source operations, CE projects, and OFCO; and ensure that all initial SAEDA reports are reviewed for exploitation UP AR 381-47 (S).

c. Retain the authority to assume direct control of an investigation or reassign it to another sub-control office when necessary. Direct case control includes imparting operational or investigative guidance, direct tasking and investigative plan approval.

d. Establish a suspense system for timely completion of priority investigations.

e. Ensure that information within the purview of other intelligence, security, or law enforcement agencies is properly referred to them, and accept and process referrals from other agencies.

f. Ensure that case files and other records/reports are properly processed and transferred to the U.S. Army Investigative Records Repository (IRR) UP AR 381-45. Close all investigations only upon files transfer to the IRR.

g. Review investigative reports for quality assurance and provide direction to the SCO for necessary corrective action.

h. Monitor the status of investigations which have been suspended or have been transferred to other agencies, but for which Army must continue an active interest.

i. Approve or disapprove requests for CI case summaries and declassification of classified case summaries, and declassify case information classified by AR 381-47(S). Coordinate with other service CI agencies and the FBI when non-Army case summaries are requested.

j. Conduct additional activities as stated in AR 381-47(S).

3-3. Sub-control offices

The SCOs are responsible for the day-to-day management of CI controlled activities conducted in overseas theaters. The SCO will be staffed by experienced CI investigative personnel. The SCO will—

a. Serve as the central focal point for and monitor the conduct of CI controlled activities within its AOR.

b. Open investigations, determine their direction and scope (except those directly controlled by the ACCO) through development and approval of investigative plans, and task investigative elements accordingly.

c. Respond to and coordinate technical direction and tasking from the ACCO.

d. Immediately report to the ACCO all incidents which meet the criteria in AR 381-12 or AR 381-47 (S).

e. Ensure that all reports have been properly addressed and disseminated based upon the content.

f. Review all CI reporting to ensure it is accurate, complete, and in compliance with CI policy and intelligence oversight.

g. Coordinate activities with legal and intelligence oversight officials, as required.

h. Refer information within the purview of other intelligence, security, or law enforcement agencies in the AOR as required.

i. Coordinate briefings to commanders and senior intelligence officials.

j. Pass lateral leads to other SCO when required, with information copies to the ACCO.

k. Complete and terminate activities and transmit final reports to the ACCO for case closure. Provide ACCO-approved summaries of information, when required, to the concerned commander and/or other agencies in the theater.

l. Forward requests for CI case summaries, non-Army case summaries, and requests for declassification to the ACCO.

m. Ensure appropriate coordination with and keep the respective senior intelligence officer informed of CI controlled activities affecting theater security.

n. Conduct additional activities as stated in AR 381-47 (S).

Chapter 4 Counterintelligence Investigations

4-1. General

a. All CI investigations will be technically controlled by one of the control offices as stated in chapter 3.

b. Conduct all investigations UP AR 381-10 and this regulation, AR 195-6, AR 381-12, AR 381-14(S) or AR 381-47(S), as applicable.

c. Coordinate investigations with other intelligence and law enforcement agencies as required.

d. Continue investigations until allegations are resolved; adequate information is provided to responsible officials for determining judicial, nonjudicial, administrative, or policy actions; or the ACCO decides that the investigation may be suspended, terminated, or closed.

e. CI investigations will be conducted only by personnel assigned/attached to units with a CI investigative mission, who have been school-trained in and hold specialty skill identifier (SSI) 35E, or military occupational specialty (MOS) 351B or 97B, and have been issued badges and credentials; or by Army civilian employees in career field 0132 who are assigned to CI investigative duties, have been school-trained, and are issued badges and credentials.

f. Local national investigators employed by an overseas Army CI unit, who have been issued Military Intelligence (MI) representative credentials, may conduct investigative leads. They will not be the primary or sole investigators.

4-2. Investigations under Army CI jurisdiction

a. CI investigative jurisdiction is derived from national, DOD, and Army policy that defines the types of incidents and personnel who are subject to investigation by Army CI components.

b. Army CI jurisdiction includes the following:

(1) Treason.

(2) Espionage and spying.

(3) Subversion.

(4) Sedition.

(5) FIS-directed sabotage.

(6) CI aspects of terrorist activities directed against the Army.

(7) CI aspects of assassination or incapacitation of Army personnel by terrorists or by agents of a foreign power.

(8) Investigation of the circumstances surrounding the defection of military personnel, and DA civilians overseas, and debriefing of the individual upon return to U.S. control.

(9) Investigation of the circumstances surrounding the detention of DA personnel by a government or hostile force with interests inimical to those of the United States.

(10) Investigation of the circumstances surrounding military members, and DA civilians overseas, declared absent without leave (AWOL), missing or deserters, who had access within the last year to TOP SECRET national defense information or sensitive compartmented information (special category absentees) (SCA); who were in a special mission unit (SMU); who had access to one or more special access programs; or were in the DA Cryptographic Access Program (DACAP); and debriefing of these personnel upon return to U.S. control.

(11) CI aspects of security violations; known or suspected acts of unauthorized disclosure of classified information or material; unauthorized access to DA computer systems; and COMSEC insecurities. These CI investigations may occur simultaneously with the command's own responsibilities under AR 380-5.

(12) CI aspects of incidents in which DA personnel with a SECRET or higher security clearance, access to a SAP or sensitive compartmented information, or in the DACAP or an SMU, commit or attempt to commit suicide.

(13) CI aspects of unofficial travel to designated countries, or contacts with foreign diplomatic facilities or official representatives, by military personnel or by DA civilians overseas.

(14) CI investigations of CI scope polygraph examinations and refusals as specified in appendix E.

c. Within the United States, Army CI has investigative jurisdiction over the following persons:

(1) U.S. Army personnel on active duty.

(2) Retired Army military personnel when the act(s) under investigation took place while the individual was on active duty.

(3) Active and inactive members of the U.S. Army Reserve Components, when the act(s) under investigation took place while the individual was in military duty status.

(4) Active, retired, and Reserve Components personnel of other services, where DOD has given Army CI geographic jurisdiction.

d. Outside the United States, Army CI has investigative jurisdiction over the following persons (unless responsibility is otherwise assigned by U.S. law, executive directive, or agreement with the host government):

(1) Army personnel on active duty and their family members.

(2) Current DA civilian employees, including foreign national employees, and their family members.

(3) Army contractors and their family members, subject to coordination with the FBI, CIA, and host government agencies.

(4) Retired Army personnel, Reserve Components personnel, and other U.S. persons, subject to coordination with the FBI, CIA, and host government agencies.

(5) Foreign nationals who are applicants for Army employment, are Army employees, or are former Army employees, no matter whether they have, require, or had access to U.S. classified information, unless responsibility is otherwise assigned by U.S. law, executive directive, or agreement with the host government.

(6) Foreign nationals not affiliated with the Army, subject to coordination with the CIA and agreements with the FBI, other DOD intelligence components and host nation governments. These investigations are under the auspices of SOFA agreements and are bilateral investigations.

(7) Active, retired, and Reserve Components personnel of other services, DOD civilian employees and family members, and DOD foreign nationals, where DOD has given Army CI geographic jurisdiction.

e. In any case, Army CI may take investigative actions necessary to—

(1) Establish the basis for administrative or nonjudicial action.

(2) Protect the security of DA personnel, information, functions, activities, and installations.

(3) Provide Army, DOD, and Department of Justice (DOJ) officials with information to help them in determining whether further investigation for prosecutorial action is warranted.

(4) Provide assistance to the FBI or security service of a host government, in support of CI investigations for which DOD is not assigned investigative responsibility.

f. Army CI jurisdiction includes both the investigation of known or suspected acts (incident investigations), and the investigation of personnel believed to be involved in those acts (personal subject investigations). Before a CI investigation can be opened, the control office must determine first, that the incident, and second, that the subject, are under Army CI investigative jurisdiction. When the subject is not known, an Army incident investigation will be conducted, in coordination with other CI investigative agencies, until the subject is identified. If the subject is under Army CI jurisdiction, it will continue as a personal subject investigation. If not, the investigation will be referred to the appropriate agency.

4-3. Personnel security investigations

a. Army CI elements will conduct personnel security investigations (PSI) overseas. PSI will be conducted under DIS direction and control.

b. All personnel conducting PSI will be evaluated under the DIS courtesy letter program, as implemented in appendix D.

4-4. Reporting requirements

a. CI elements will report to the ACCO and theater SCO all incidents which fall under the criteria of paragraph 4-2 above, AR 381-12, AR 381-14(S) or AR 381-47(S), within 72 hours of receipt of the initial information.

b. CI personnel will report immediately to the appropriate law enforcement agency all incidents which come to their attention regarding possible violations of non-national security statutes or information that suggests an immediate threat to life or property.

c. Overseas SCO will advise, and coordinate investigative activities with the appropriate FBI legal attache when an investigation is opened on a U.S. person not subject to the UCMJ.

4-5. Shared investigative responsibility and joint investigations

a. Certain national security crimes investigations may present situations where MI and USACIDC have concurrent responsibilities. MI's responsibility is to investigate such incidents for violation of national security; USACIDC's responsibility is to investigate crime within the Army. MI and USACIDC, with USACIDC as the lead agency, will share investigative responsibilities for actual or suspected incidents of sabotage and terrorism, until FIS involvement is ruled out. MI and USACIDC will jointly investigate computer intrusions until FIS involvement is ruled out. Violations of the Intelligence Identities Protection Act, section 421, title 50, United States Code (50 USC 421) may require MI as the lead agency (for example, selling identities to benefit a foreign power) or USACIDC, depending upon the circumstances. The lead agency will keep the other informed of the case progress, but will continue the investigation until it is resolved. The lead agency will turn over the case if it is later determined to be in the other's jurisdiction.

Should disputes arise, or should security considerations preclude local coordination, refer the matter to HQDA (DAMI-CIC) and HQ, USACIDC (CIDC-OP) for resolution.

b. Installation provost marshals (PM) are responsible for non-CI aspects of special category absentee investigations (para 4-2*b*(10)). Army CI will assist the PM's investigative task force to determine if there is evidence of FIS involvement or evidence of actual or potential defection; and assist the commander in determining whether there was loss or compromise of classified information/materiel. Upon return of the SCA to military control, CI will conduct a debriefing to find out if the SCA visited or entered any foreign diplomatic establishment, traveled to a country other than the one in which the SCA was stationed, had any contact with FIS, or provided sensitive or classified information or materiel to an unauthorized person. If the SCA was a defector, conduct the debriefing as outlined in paragraph 6-6.

c. Where Army CI has geographic jurisdiction, it will be the lead agency. The ACCO and SCO will ensure the parent service CI agency and/or the FBI, as appropriate, are kept informed of the case status. Investigative leads outside the geographic area will be referred to the appropriate parent service CI agency or the FBI.

d. When Army interests are involved, but subject jurisdiction rests with another agency, Army CI may request a joint investigation. Otherwise, activity will normally consist of liaison with the primary agency, providing assistance as required and authorized, and acquiring copies of reports collectable under AR 381-10. Should agencies with subject jurisdiction request assistance or a joint investigation, Army CI elements will forward the request through the responsible SCO to the ACCO for validation and coordination with appropriate legal and intelligence oversight personnel. Upon ACCO validation, Army case control procedures will reflect an Army CI investigation.

4-6. Jurisdiction over Army personnel at U.S. missions abroad

The FBI has overall responsibility for the conduct of espionage investigations at U.S. embassies and other diplomatic establishments outside the United States.

a. The FBI will either supervise the conduct of, or actually conduct such investigations. Army CI will ensure that the FBI is informed of Army interests when Army personnel are the subjects or Army information is involved.

b. The FBI may choose to establish an investigative team which includes Army CI, or may choose to use Army CI assets rather than send an FBI team overseas. In either case, Army case control procedures will reflect an Army CI investigation.

c. If the FBI decides to terminate or not to open an investigation where Army personnel are involved, Army CI may investigate, as stated in paragraph 4-2*d*. The investigation will be conducted in consultation with the FBI, and the FBI will be advised if possible violations of espionage statutes are uncovered.

4-7. Impersonation of DA military intelligence personnel or the fabrication, unauthorized possession or use of military intelligence documentation

a. Impersonation of military intelligence personnel, fabrication of intelligence badges and credentials, and unauthorized possession or use of actual badges and credentials are violations of section 701, title 18, United States Code (18 USC 701), section 912, title 18, United States Code (18 USC 912), and Article 134, UCMJ. Investigations of such allegations are the responsibility of USACIDC or the FBI.

b. CI will maintain an active interest in the investigation, as stated in paragraph 4-5*d*. Should evidence of FIS involvement surface, a joint investigation will be requested.

4-8. Use of the National Crime Information Center (NCIC)

a. All CI investigative elements will use the NCIC wherever possible. On military installations, these terminals are under the control of the installation provost marshal or security officer.

b. Use of the NCIC will be in accordance with AR 190-27, 190-30, FBI operating instructions, and local PM/security officer procedures.

c. Overseas CI elements may request NCIC checks through a lead to ACCO, if an NCIC terminal is not available.

d. Information obtained from NCIC checks will be handled in accordance with AR 381-10.

4-9. Release of investigative information

a. Investigative information may be released to other CI or law enforcement agencies when the information is within their jurisdictions. Release of investigative information to other agencies will occur only upon approval by the ACCO.

b. The information will be provided in a Summary of Information (SOI) report. SOI will summarize only the information relevant to the receiving agency. SOI will not include internal Army taskings, coordinations, or comments; source identifying data; or Army CI modus operandi.

c. The SCO or ACCO will produce or direct production of SOI, as appropriate.

Chapter 5 Counterintelligence Operations and Techniques

Section I Counterintelligence Special Operations

5-1. General

CI special operations are those which are generally carried out under the auspices of the National Foreign Counterintelligence Program, and involve direct or indirect engagement with FIS through human source or technical efforts. CI special operations are governed by AR 381-47(S), and consist of—

- a.* Offensive counterintelligence operations.
- b.* Counterespionage projects.
- c.* Defensive source programs.

5-2. Operations

a. Offensive counterintelligence operations will be conducted only by INSCOM and the 650th MI Group.
b. Defensive source program operations, designed to protect designated Army activities against a confirmed HUMINT threat, are conducted only by those agencies approved by HQDA in classified implementing memoranda.

Section II Counterintelligence General Operations

5-3. General

General operations are essentially defensive in nature and are aimed at supporting the force protection programs and formal security programs of Army commanders at all levels.

5-4. CI support to force protection

a. Force protection is a command responsibility. To carry out force protection responsibilities, the commander requires support from several sources, one of which is the intelligence community.

b. CI support to force protection will be tailored to the sensitivity of the supported organization and its vulnerability to FIS collection and hostile attack. This support can be tailored from a combination of CI activities as described in this and other CI publications, and may include—

- (1) CI support to mobilization security, including ports and major records repositories.
- (2) CI support to combatting terrorism.
- (3) CI support to rear operations.
- (4) CI support to civil-military affairs.
- (5) CI support to psychological operations.
- (6) CI support to battlefield deception.
- (7) CI support to operations security.
- (8) CI support to friendly communications-electronics (C-SIGINT).

c. Countermeasures recommendations by supporting CI elements are not directive in nature, unless provided for in other regulations or endorsed as such by the supported commander. The priority, risks, and resource allocation decisions to implement countermeasures are the supported commander's responsibility.

5-5. Low level source operations (LLSO)

Low level source operations support force protection of deployed U.S. forces. LLSO are governed by classified HQDA implementing memoranda.

5-6. Advice and assistance

CI advice and assistance are technical consultations aimed at improving or sustaining force protection and formal security programs. These consultations aid the security manager in developing or improving security plans and standard operating procedures. Such assistance can be programmed or unprogrammed. It can include, but is not limited to—

- a.* Advice concerning the conduct of inspections, security planning, the resolution of security problems, or development of classification guides;
- b.* Conduct of CI surveys, technical inspections, and preconstruction technical assistance;
- c.* Conducting SAEDA training, providing SAEDA materials, and training security managers ("train the trainer") in the SAEDA program;
- d.* Providing investigative advice to the command's security investigations under AR 15-6 and AR 380-5.

5-7. Counterintelligence technical support activities

a. Technical support activities are specialized subdisciplines of counterintelligence. They are governed by separate regulations as listed below:

- (1) Technical Surveillance Countermeasures (TSCM), AR 381-14(S).
- (2) Intelligence polygraphs, AR 195-6 and this regulation.

b. Although TSCM are specialized investigations and polygraph is an investigative technique, they also have applications in general operations. INSCOM and the 650th MI Group conduct TSCM. INSCOM conducts intelligence polygraphs.

5-8. CI support to acquisition and special access programs

a. INSCOM conducts CI support to Army RDTE and acquisition elements through the Acquisition Systems Protection Program (ASPP). The ASPP assesses FIS technical options for countering U.S. weapons systems. The program's goal is to protect the U.S. technical lead by conducting counterintelligence support throughout the acquisition process.

b. SAPs generally involve either military acquisition, a military operation, or intelligence activity. CI support to SAPs will extend, as applicable, to Government and industrial security enhancements; to DOD contractors and their facilities, in coordination with DIS as appropriate; and to the full range of sensitive RDTE activities, military operations, and intelligence activities for which DA is the proponent or executive agent.

c. INSCOM is responsible for providing life cycle CI support to approved SAPs and for maintaining the capability and expertise to meet Army needs for CI support to SAPs. CI support will automatically be provided to Secretary of the Army approved category I and II SAPs, and selected DOD and category III SAPs as approved by HQDA (AR 380-381).

5-9. CI support to HUMINT

CI support to HUMINT ensures the integration of the two disciplines. CG, INSCOM will ensure HUMINT and CI staffs review each other's plans for possible compromise, passing a source from one to the other, or investigative requirements.

5-10. CI support to treaty verification

a. Arms control treaties have resulted in an overt FIS presence at U.S. facilities. CI is primarily concerned with non-treaty related aspects of overt FIS visits to Army installations, to protect installation activities and facilities not subject to treaty verification. CI personnel provide advice and assistance to installation commanders, and debrief Army personnel who may have come in contact with inspectors.

b. Within CONUS, INSCOM is responsible for CI support to treaty verification, with FORSCOM support. Liaison with other U.S. agencies involved in the treaties will be in accordance with paragraph 5-11*a*.

c. Outside CONUS, all CI elements will provide CI support to treaty verification, as directed by the affected unified, specified, or allied command CINC.

5-11. Liaison

a. Liaison is used to exchange information, obtain assistance, and prevent duplication of effort. It includes overt collection of intelligence information. Collection, use or dissemination of information gathered through liaison will comply with AR 381-10.

b. Within the United States—

(1) The ODCSINT is responsible for liaison with the national headquarters of all Intelligence Community and other agencies on CI policy matters or commitments. Except as provided in this regulation, or as otherwise authorized, communications with those national agency headquarters will be handled only through ODCSINT.

(2) The CG, INSCOM will provide a single point of contact liaison with the national headquarters of FBI and other federal agencies for coordinating CI operational and investigative matters. INSCOM CI elements will conduct continuing liaison with federal regional offices, other military intelligence services, state and local authorities as essential to support CI activities.

(3) CI elements of non-INSCOM MI units located in the United States will conduct on-post liaison activities and off-post liaison with local authorities as necessary to accomplish their assigned CI responsibilities. Prior to conducting off-post liaison, coordination will be made with the nearest INSCOM CI element, to determine if the desired information is already available, to avoid duplication of effort, and to facilitate information sharing. If appropriate, memoranda of understanding may be developed between INSCOM and the affected MACOM, which will formalize information exchange and include limits of liaison activities.

c. In overseas areas, MACOM commanders will establish CI liaison programs with other U.S. and foreign agencies, consistent with the following:

(1) To avoid confusion and duplication, intelligence components that desire CI liaison with foreign agencies will first determine if another element is performing the needed liaison. If so, attempts should be made to obtain the desired

data through agencies with existing liaison. If new arrangements or changes to existing arrangements with foreign agencies are required, coordinate them UP AR 381-171.

(2) Operational and strategic CI units, and CI elements of SMU and Special Operations Forces units, will conduct continuing liaison with the United States, host and other foreign government intelligence agencies, and law enforcement agencies as essential to support CI activities.

(3) Tactical CI units will conduct continuing liaison with military law enforcement elements, and liaison with appropriate police and security agencies as required for wartime planning. In coordination with the theater MI unit, they will conduct the latter liaison often enough to ensure a smooth transition to full wartime liaison. Conduct continuing liaison with theater MI units to obtain CI information that may impact upon the command.

5-12. CI support to domestic civil disturbances

At the direction of the supported CINC, military personnel may be deployed to support civilian law enforcement agencies (LEA) during domestic civil disturbances. Since EO 12333 and AR 381-10 do not apply to law enforcement activities, any activity by CI personnel must comply with the following:

a. The primary CI function is to support unit force protection efforts, through close and continuous liaison with civilian LEA. Civilian LEA are the primary information collectors and files retention agencies. With certain narrow exceptions, CI personnel may conduct collection activities only after Secretary or Under Secretary of the Army approval. The activities must comply with DOD 5200.27 and AR 380-13.

b. CI personnel may provide additional support only after coordination with the task force senior intelligence officer and legal advisor, and have prior approval by the task force commander's designated law enforcement representative. This support may include investigative skills, analysis of criminal information, and situation development.

c. All CI personnel involved will be in uniform, and MI badges and credentials will not be used.

d. All CI personnel alerted for possible deployment must understand the sensitivities concerned with past deployments of Army CI assets in domestic civil disturbance situations. Take every precaution to ensure CI personnel do not conduct any activities without prior approval, and do not collect or maintain information on U.S. persons beyond that specifically authorized for the deployment duration.

5-13. CI support to natural disaster operations

At the direction of the supported CINC, CI personnel may be deployed to assist in natural disaster operations. They remain under the provisions of EO 12333 and AR 381-10. Without an identifiable threat to U.S. security interests, however, use of CI personnel is not recommended.

Section III

Counter-Signals Intelligence (C-SIGINT)

5-14. General

a. C-SIGINT systematically examines friendly C-E signals and systems to determine their susceptibility to electronic exploitation.

b. C-SIGINT may be employed as an independent service, or in conjunction with other operations to provide an all-source multidisciplined vulnerability assessment.

5-15. Counter-SIGINT support

a. C-SIGINT collection and analysis, including COMSEC monitoring (AR 380-53), will be performed at operational and theater levels to enhance force protection, survivability, mobility and training; and to provide empirical data to identify friendly C-E vulnerabilities and provide the basis for countermeasures recommendations.

b. Theater C-SIGINT resources will provide service to acquisition and SAPs; special operations forces; the Army component of joint, unified, and specified command exercises and operations; and other DOD activities as required. Emphasis should be placed on the following:

(1) Developing and maintaining detailed databases on FIS electronic collection and targeting capabilities.

(2) Collecting, analyzing, and maintaining data, in fixed and mobile environments, on critical C-E nodes that directly support a unit's command, control, communications and intelligence system; and systems that exhibit unique external signal parameters, signal structures, and modulation schemes that could allow FIS to identify, track, or target friendly elements.

(3) Collecting operational signals to measure the degree of security achieved by U.S. codes and cryptographic equipment.

(4) Assessing the types and value of information subject to loss through intercept and exploitation of friendly telecommunications.

(5) Determining the effectiveness of electronic protection, electronic attack, cover and deception activities, and operations security measures.

Section IV Techniques

5–16. General

a. Counterintelligence techniques are those means used to accomplish the mission most efficiently and effectively. The selection of CI techniques to be employed will be determined at the lowest possible level by the on-scene CI element in conjunction with the supported military commander, within the constraints of the operation and applicable regulations.

b. General types of CI techniques are explained in the following paragraphs. This list is not all-inclusive. Detailed techniques are found in FM 34–60 and FM 34–5 (S/NF).

5–17. Vulnerability assessments

a. Vulnerability assessments are studies conducted by CI personnel to provide a supported command or agency a picture of its susceptibility to foreign intelligence collection. These assessments may be conducted on a command, agency, installation, subordinate element, headquarters, operation, or program, and are tailored to the needs of each requestor.

b. The objective is to provide a supported command or agency a realistic tool with which to evaluate internal force protection or security programs, and to provide a decisionmaking aid for the enhancement of these programs. Vulnerability assessments include the following:

- (1) Evaluation of FIS multidiscipline intelligence collection capabilities, collection and other activities, and priority intelligence requirements.
- (2) Identification of friendly activities patterns (physical and electronic), friendly physical and electronic signatures, and the resulting profiles.
- (3) Monitoring or collecting C-E transmissions/signatures to aid in vulnerability assessments, and to provide a more realistic and stable basis from which to recommend countermeasures.
- (4) Identification of vulnerabilities based upon analysis of collected information, and recommendation of countermeasures.
- (5) Analyzing the effectiveness of implemented countermeasures.

5–18. Hostile intelligence simulation (Red Team)

a. Upon request by a commander or program manager, CI personnel may plan and execute a simulation of a foreign intelligence penetration of a specified target, such as an installation, operation, or program. Such simulations are informally known as “Red Team operations.”

b. Red Team operations should be carried out as realistically as possible, but within the provisions of AR 381–10.

c. When using C–SIGINT resources to support Red Team operations, commanders will ensure compliance with the regulatory provisions governing the use of assets to perform electronic collection.

d. Because of the complexity and high resource requirements, Red Team operations should generally be limited to extremely sensitive activities, such as SAPs, although Red Team operations may be useful in conjunction with major tactical exercises and deployments.

e. Red Team proposals will be documented in an operations plan and approved by the activity head or commander who requested the service.

5–19. Covering agent support

CI covering agent support is the technique of assigning a primary supporting special agent to a command or agency. This agent will conduct all routine liaison and 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 designated point of contact for reporting matters of actual or potential CI interest.

Chapter 6 Counterintelligence Collection

6–1. General

a. Collection and reporting of intelligence information is a continuing requirement at all Army levels and is both authorized and directed by Executive Order, DOD and Army regulations.

b. National-level collection requirements for intelligence information are validated and issued by the Defense Intelligence Agency (DIA). These consist of—

- (1) Information objectives.
- (2) Time sensitive collection requirements.

(3) Source-directed requirements.

(4) Collection emphasis requests.

c. Operational and tactical level requirements are validated and issued by collection managers at the appropriate level. Where such requirements also respond to a national collection requirement, they will be reported to national level.

d. Collection will be conducted in accordance with policy established in AR 381-10. Additionally, the 650th MI Group will comply with ACE directives.

6-2. Identifying and validating collection requirements

Guidelines for validating collection requirements for counterintelligence information are in FM 34-5 (S/NF).

6-3. Collection and reporting procedures

a. Army CI elements will collect and report military and military-related foreign intelligence and CI information on FIS requirements, capabilities, operations, and modus operandi; espionage; other intelligence activities; sabotage, assassination and computer intrusions when FIS involvement is suspected; terrorist activities; subversion; sedition; FIS involvement in unauthorized technology transfer; and the foreign aspects of narcotics production and trafficking in accordance with validated collection requirements, assigned priorities, and resource capabilities.

b. Army CI elements will report information responsive to collection requirements in Intelligence Information Report (IIR) format. FM 34-5(S/NF) contains format details. They will limit dissemination to production elements, headquarters, and organizations having a direct interest in the information. They will send the original IIR to DIA, with an information copy to USAITAC and a copy of terrorism-related IIR to the ATOIC; and sanitize IIR information to preclude compromise of sensitive operations or investigations. When the situation dictates, reporting elements may invoke the Originator Controlled (ORCON) caveat IAW DCID 1/7 to ensure restricted dissemination.

c. Information derived from potential or on-going CI investigations, concerning FIS modus operandi, systemic threats, or known compromise of information, may be reported in IIR, after ACCO approval. The report will be sanitized to protect the integrity of the investigation.

d. All Army commanders who become aware of information that is or may be of CI interest, as indicated in paragraph 4-2b, will promptly report this information via secure channels to the supporting Army CI element.

e. CI elements will ensure the rapid exchange of information outside immediate command channels. CI elements that obtain raw information related to force protection will immediately forward that information to the affected commander, and to analysis and production centers through IIR.

f. CI elements which incidentally acquire international narcotics information, reasonably believed to indicate a violation of federal law, will report it to the applicable drug law enforcement agency within 5 working days of discovery. Information which meets a valid collection requirement will be reported through IIR.

6-4. Local operational data

Local operational data is that which responds primarily to local MI requirements or is of interest only to local area commands, such as force protection information derived from low level source operations. Some of this information may also respond to validated collection requirements of other intelligence consumers, and will be reported by IIR. Otherwise, local operational data will be analyzed and added to data bases as required. No CI investigation will be conducted under the guise of local operational data collection.

6-5. Debriefings and interrogations

a. Debriefing defectors and returned U.S. prisoners of war or hostages can yield information on the personalities, modus operandi, and organization of FIS, terrorists, and other political extremists. Interrogations of enemy prisoners of war and civilian internees can yield significant information of CI interest, as well as combat information.

b. Debriefings of returned U.S. prisoners of war and hostages, and general interrogations are primarily done by interrogators responding to validated collection taskings. Depending on technical requirements, they may be done by CI personnel and interrogators together, in accordance with established joint procedures.

6-6. Returned U.S. defector debriefings

a. Returned U.S. defectors are of CI interest for any knowledge they may have of other U.S. defectors and of FIS personnel. These debriefings may provide leads to defectors who had access to classified information or who may have worked for FIS before or after defection.

b. Upon notification of a U.S. defector's return, CI agents will debrief the defector for the following:

(1) Persons and organizations with whom the defector came into contact or who provided assistance during his absence. Agents will obtain complete identity and physical description of individuals, and the name and type of organizations.

(2) The source of funds while en route and at destination.

- (3) Whether or not the defector used an alias or otherwise concealed his identity. If so, complete details, including the means of acquiring any false identification, should be determined.
 - (4) The identification and disposition of military equipment taken with the defector.
 - (5) The means of crossing national boundaries, documentation required, and difficulties encountered.
 - (6) Complete details of any debriefings or questioning the defector underwent to include the matters discussed, the interrogator's attitude (that is, whether friendly or hostile), the extent of the defector's cooperation, and the interrogator's reaction to any refusal to answer questions. The agent will elicit the identity and physical description of any interrogators to the maximum extent possible.
 - (7) Any attempts to solicit the defector's assistance in any way, such as requesting additional information on any person or organization, reestablishing contact at a later time, or FIS offers to employ the defector.
 - (8) The nature and extent of any publicity given to his travels or residence.
 - (9) The attitude of the foreign government to the defector's presence, including the way in which this position was expressed or displayed.
 - (10) Complete details of any contacts with other U.S. defectors. This should include identifying data, descriptions, military unit (if any), last known location, and known or suspected activities, especially cooperation with or employment by FIS.
 - (11) Identifying data, descriptions, activities, and last known location of known or suspected FIS personnel.
- c.* The primary purpose of a defector debriefing is information gathering. Nonetheless, every returned defector will be advised of their rights under Article 31(b) of the UCMJ since, at the minimum, they are usually suspected of violation of Article 85, Desertion. Debriefing agents should consult the local staff judge advocate (SJA) for advice on specific offenses the defector is suspected of violating. Additional guidance for tailoring the debriefing may be obtained from the SCO/ACCO.
- d.* Information gained from these debriefings may be reportable in an IIR, unless it is an investigative lead. Debriefing agents should contact the SCO/ACCO for guidance.

Chapter 7

Counterintelligence Analysis and Production

7-1. General

USAITAC conducts analysis and production of strategic CI information. All echelons where CI staff capability exists conduct CI analysis and production to meet local needs.

7-2. Analysis

a. CI analysis focuses on foreign intelligence and security services, to limit the effectiveness of foreign multidiscipline collection and targetting of information on Army operations, activities, technology, and intentions. Raw information, open source material, and finished intelligence products will be analyzed in response to local and national requirements. Finished intelligence products are not limited to those produced by the Army, but include those produced by other services, the FBI, the CIA, other federal intelligence and law enforcement agencies, DOD contractors, and allied intelligence, security and law enforcement agencies.

b. CI analytical elements will maintain threat and friendly data bases from which an analytical product may be derived. The databases may include aFIS order of battle, FIS readiness and capability data, limitations, FIS priority intelligence requirements (PIR), friendly PIR and essential elements of friendly information (EEFI), biographical data on significant FIS personalities, FIS collection events and modus operandi, friendly operational profiles, friendly vulnerability data, and historical data on countermeasures implementation and outcome.

c. Strategic CI analysis may include—

- (1) Analysis in support of national and Army programs and decision making.
- (2) Compilation of local analysis into global assessments.
- (3) Trends in FIS modus operandi and collection priorities.
- (4) Assessments of FIS technical options for countering U.S. weapons and intelligence systems.
- (5) Impact of technology transfer activities on the U.S. military's technical lead.

d. Local CI analysis may include—

- (1) Threat analysis considering the vulnerabilities of the commanda anda tailored assessments of the threat as related to force protection and security programs.
- (2) Supporting analyses to battlefield deception and command, control, and communications countermeasures activities.
- (3) Portrayal of the friendly situation as seen by the opposing commander through his intelligence capability. Such analysis will also consider the influence of that assessment on the opposing commander's decisions.

7-3. Production

- a.* Strategic CI production includes—
- (1) Assessments in support of national and Army programs, SAPs, and acquisition programs.
 - (2) Worldwide assessments of the organization, location, funding, training, operations, capabilities, and intentions of terrorist organizations.
 - (3) Global trends in FIS modus operandi to permit integration of pertinent information into the Army's SAEDA education program.
 - (4) Studies and assessments in response to national derivative or delegated production requirements.
 - (5) After action studies of individual cases of espionage against the Army.
 - (6) Analyses of the intelligence collection capabilities of international narcotics trafficking organizations, when DIA assigns a production task to Army.
 - (7) Multimedia threat products to support Army CI awareness programs.
- b.* Local CI production includes, but is not limited to, the following:
- (1) Current intelligence.
 - (2) CI threat or vulnerability analyses tailored to specific activities, units, installations, programs, or geographic areas.
 - (3) CI studies to support contingency planning and major exercises.
 - (4) Studies of FIS organization, methods of operation, personnel, activities, and intentions that pose a current or potential threat to the supported command.
 - (5) Assessments of the organization, location, funding, training, operations, capabilities, and intentions of terrorist organizations.
- c.* Because these products contribute significantly to USAITAC's strategic analysis, information copies of MACOM CI production will be provided to USAITAC.

Chapter 8

Employment, Use, and Special Administration of U.S. Army Counterintelligence Personnel and Authority of CI Special Agents

Section I

Employment, Use, and Special Administration of U.S. Army Counterintelligence Personnel

8-1. Personnel involvement

Elements affected by policy in this chapter are—

- a.* Active Army and RC elements to which CI personnel are assigned or attached.
- b.* Personnel with SSI 35E or MOS 351B, 97B or 97G, as a primary or additional specialty, or those who are assigned to duties in those positions.
- c.* DA civilian employees in GS-0132, assigned to CI investigative, operational, or liaison duties.

8-2. Assignment of CI personnel

Counterintelligence is a controlled specialty. CI personnel with a primary CI specialty as listed in paragraph 8-1 should be assigned to duties and activities that aid the CI effort. Assignment to consecutive tours in non-counterintelligence related positions, or assignment of Counter-SIGINT personnel to non-Counter-SIGINT duties, will be made only with the approval of the appropriate Personnel Management Directorate, PERSCOM or ARPERCEN.

8-3. Duty limitations

Personnel assigned to positions in units authorized an SSI, MOS, or civilian specialty as listed in paragraph 8-1, who are performing primary duties within one of these specialties—

- a.* Will not be assigned to duties outside the scope of their specialty that will either compromise the performance of their CI duties or preclude accomplishment of essential CI functions.
- b.* Will not be used to perform the following:
 - (1) Investigations of war crimes, atrocities, welfare of the civilian populace, or criminal activities not under CI jurisdiction.
 - (2) Interrogation or detention duties not connected with assigned missions and functions of the unit to which assigned or attached.
 - (3) Combat patrols and reconnaissance activities, unless CI targets are involved.
 - (4) Guard or duty officer type duties, except as required directly within the unit to which they are assigned or

attached (for example, corps/division headquarters company, MI brigade/group, divisional MI battalion, separate MI company/detachment).

(5) Housekeeping or other duties of a similar nature, except as required directly within the unit to which they are assigned or attached.

(6) Personal protective services (USACIDC responsibility).

(7) Casualty notifiers or casualty assistance officers, when normal duties require civilian clothing status.

c. Should not be detailed to perform command and administrative security investigations under AR 15-6 and AR 380-5, except for internal investigations required directly within the unit to which CI personnel are assigned or attached. Such investigations present a special problem for CI personnel, due to intelligence oversight requirements and a potential conflict of interest. CI personnel so detailed represent the command and not USAI; badges and credentials will not be used and the personnel will not imply that they are representing USAI or conducting a CI investigation. If the command investigation uncovers indications of activity under CI jurisdiction, the CI detailee will immediately report it to the SCO, and halt the command investigation to avoid a conflict of interest. Should the command wish to continue its internal investigation, it must do so in close coordination with the SCO, and with a non-CI detailee. CI personnel may provide expert advice to a command security investigation at any time.

8-4. Withdrawal of SSI/MOS/civilian specialty

a. Upon determination that an individual is no longer qualified or suitable to perform duties in counterintelligence, the commander will withdraw the individual from CI duties and recommend that the individual be removed from the Army CI Program.

b. Withdrawals for cause constitute disqualification from the CI Program. Any of the following will be considered an appropriate basis for withdrawal from CI duties for cause and revocation of the CI SSI/MOS/civilian specialty:

(1) Court-martial or other Federal or state convictions, or nonjudicial punishment. (Evaluate non-U.S. court convictions for applicability to U.S. law.)

(2) Indiscretion, breach of discipline, abuse of privilege, or the unauthorized release of information.

(3) Financial irresponsibility.

(4) Demonstrated lack of character or moral integrity necessary for proper performance of CI duties.

(5) Mental disorder verified by competent medical authority.

(6) Failure to successfully complete a CI course of instruction.

(7) Loss of badge or credentials through neglect, or repeated misuse of badge or credentials.

(8) Revocation or denial of a security clearance, or failure to maintain a current Single Scope Background Investigation, or failure to meet or maintain MOS/specialty requirements.

(9) Demonstrated inability to perform assigned duties or duties inherent in the designated skill level.

(10) An individual's request to be removed from the Army CI Program or from assignment to CI duties.

(11) Other conduct that would preclude the individual's continued performance of CI duties.

c. Specialty revocation action should not be taken until one or more of the conditions in paragraph 8-4b has been reasonably confirmed. Such investigation should be completed within 30 days and more promptly if possible.

d. Recommendations to revoke SSI/MOS will be processed through personnel channels to PERSCOM or ARPERCEN, where the final decision will be made. Recommendations for civilian removal from CI duties will be based on applicable civilian personnel policies. Send information copies to HQDA (DAMI-CIC).

e. In the absence of a commander's recommendation, PERSCOM or ARPERCEN may revoke the specialty when the individual's records indicate one or more of the conditions in paragraph 8-4b are present, pursuant to qualitative review programs.

8-5. Clothing and grade

a. Personnel assigned to CI duties will wear clothing appropriate to the mission, operation or cover as authorized by the unit commander to which assigned or attached.

b. Personnel wearing the uniform will comply with AR 670-1. Requests for exceptions to policy will be fully justified and forwarded through HQDA (DAMI-CIC) to HQDA (DAPE-MPH-S).

c. Military personnel routinely authorized to wear civilian attire in accordance with an approved cover plan will not be required to perform uniformed military duties or attend military formations that would jeopardize the cover.

d. Enlisted personnel assigned to perform duties requiring the full-time wearing of civilian clothing are entitled to the civilian clothing allowance.

e. Officers assigned to overseas positions which require the full-time wearing of civilian clothing are eligible for the civilian clothing allowance. Officers who perform TDY to an overseas area in excess of 15 days duration and are required to wear civilian clothing exclusively are authorized a partial clothing allowance appropriate to the season in which the TDY occurs.

f. Process requests for civilian clothing allowances in accordance with AR 700-84.

g. CI special agents in the conduct of CI activities are not required to reveal their military grade or position other

than as “CI Special Agent” when in civilian clothing status and when such disclosure would interfere with the proper discharge of investigative or operational duties.

8–6. Nonstandard spectacles

Issue of nonstandard spectacles to personnel assigned to SSI/MOS positions listed in paragraph 8–1*b* is authorized by AR 40–63.

8–7. Access to military privileges

CI personnel required to wear civilian clothing have medical, exchange, commissary, and other normal military privileges to which they are entitled as members of the armed forces. When required for security purposes (for example, unit mission), local procedures will be established that will permit CI personnel access to all such services, on presentation of agreed-upon identification. To protect the rights and benefits of persons concerned, essential elements of identification, properly classified, will be made a matter of record between intelligence unit commanders and agencies concerned. Thereafter, that information will be given limited dissemination on a need-to-know basis only.

8–8. Billets, mess, and temporary duty

a. General. To protect the ability of enlisted CI soldiers to perform their sensitive duties, special billets and mess may be authorized. The following provisions will apply to those CI soldiers who are certified by their commander to be performing duties where close association with non-CI personnel is likely to interfere with the accomplishment of those duties (such as billeting with personnel whom the CI soldier is investigating).

b. Billets. Single or unaccompanied CI soldiers, certified as above, must be billeted with other CI or USACIDC personnel in facilities separate from other soldiers not assigned to those type units. When such facilities are not available, they will be billeted in Senior Enlisted Quarters, officer quarters, or be given statements of nonavailability.

c. Mess. When commanders have identified personnel assigned to CI duties, whose use of a messing facility would adversely affect those duties, a blanket request for authorization of Rations Not Available will be submitted to the Commander, U.S. Army Finance and Accounting Center, ATTN: SAFM–FAP–PE, Indianapolis, IN 46249–1006, in accordance with the DOD Military Pay and Allowances Manual.

d. Temporary Duty (TDY). CI personnel, when certified by their commanders to be performing CI investigative or CI special operational duties in a TDY status, will not be billeted in troop transient billets or be required to use a Government mess when such use would be detrimental to the mission. TDY orders will reflect that the use of Government billeting and mess facilities would be detrimental to the mission.

e. Applicability. These provisions apply both overseas and within the United States.

8–9. Weapons

a. CI personnel may carry weapons openly or concealed as required in the performance of peacetime official duties, in accordance with AR 190–14, when authorized by a field grade officer. Commanders will ensure the individual has met the requirements of AR 190–14 and weapons qualification requirements. Weapons storage will comply with current regulatory requirements.

b. During deployments, crisis, transition to war, and hostilities, CI personnel will carry weapons as authorized and required by unit mission.

Section II

Authority of CI Special Agents

8–10. Freedom of movement

If emergency circumstances preclude advance notification, CI special agents assigned to another theater are not required to obtain specific theater clearance from overseas commanders prior to undertaking overseas travel in connection with their official duties. (See AR 1–40, para 1–2*b*(5).) In such cases, the senior intelligence officer of the Army theater component command will be notified as soon as possible of the travel.

8–11. Oath administration

A CI special agent is authorized to administer oaths when taking statements. The agent’s title for oath administration is “Counterintelligence Special Agent, U.S. Army.” Authorities are the Uniform Code of Military Justice (UCMJ), Article 136(b) for military and 5 USC 303(b) for civilian special agents.

8–12. Apprehension authority

a. Pursuant to 10 USC 807–809, 28 USC 535, Rules for Courtmartial (RCM) 302, AR 600–40, and this regulation, CI special agents are authorized to apprehend any person subject to the UCMJ, regardless of location, if there is a reasonable belief that the person has committed a criminal offense under USAI investigative jurisdiction. CI special agents are also authorized to conduct investigative stops of any person subject to the UCMJ, regardless of location, if there is a reasonable suspicion that the person has committed a criminal offense under USAI investigative jurisdiction.

b. CI special agents are authorized to detain civilian personnel on military installations or facilities when there is a reasonable belief that the person has committed a criminal offense against the U.S. Army, and that offense is within USAI investigative jurisdiction. CI special agents are also authorized to conduct investigative stops of civilians on military installations or facilities, if there is a reasonable suspicion that the person has committed a criminal offense under USAI investigative jurisdiction. Civilians will be detained only until they can be released to the FBI.

c. Army CI special agents may not apprehend or detain civilians outside the limits of a military installation or facility within the United States. When an apprehension is necessary in the conduct of a CI investigation, an arrest warrant must be obtained and executed by a civil law enforcement officer. CI special agents may accompany the arresting official for the purpose of identifying the person to be arrested and to provide assistance as authorized in AR 500–51.

d. Apprehension of civilians off a military installation or facility outside the United States may be authorized if host nation authorities consent and the proper arrest warrant is obtained.

e. Personnel apprehended by CI special agents will be released to civil or military police, as appropriate, for processing, detention, or confinement.

8–13. Search and seizure authority

a. Searches and seizures within the confines of a U.S. military installation or facility will be conducted in accordance with the Military Rules of Evidence, Manual for Courts-martial (MCM); AR 190–22; or other applicable policy.

b. Searches and seizures outside a military installation or facility in the United States will be conducted in accordance with Rule 41, Federal Rules of Criminal Procedure, 28 CFR 60, and AR 190–22. Coordination with the supporting staff judge advocate and concurrence of the appropriate U.S. Attorney are mandatory prior to seeking a civil search warrant. CI special agents may accompany the civil law enforcement official, who will actually execute the search warrant.

c. Searches and seizures outside a military installation or facility outside the U.S. are subject to SOFA.

8–14. Involvement in civil legal proceedings

Requests for the appearance of CI special agents at depositions or in civil proceedings and for the subpoena of information exempt from release to the public will be processed in accordance with AR 27–40.

8–15. Access to records, information, and facilities

a. Upon presentation of the MI badge and credentials or MI representative credentials, CI special agents and CI assistants will be permitted access to Army records under the provisions of AR 340–21, as required for the conduct of CI investigations or operations. They are also authorized to make extracts or transcripts of specific information obtained from the records custodian. The actual records will remain under the control of the records custodian, who will make either the records or legible certified copies available for judicial, non-judicial, or administrative proceedings.

b. Access to private sector financial records is authorized under 12 USC 3401–3419, 15 USC 1681f, and AR 190–6, provided that the required notifications or exceptions have been executed.

c. Access to records of other Federal agencies is provided for under 5 USC 552.

d. CI special agents and CI assistants will be granted access to all Army facilities when necessary for CI investigations or operations, consistent with the applicable security directive and the individual's access. Persons presenting Special Agent badge and credentials possess a final TOP SECRET security clearance based on a Single Scope Background Investigation.

8–16. CI special agents assigned to Special Mission Units

CI special agents who are authorized the MI badge and credentials, and who are assigned to SMU, may also be issued the SMU badge and credentials at the SMU commander's discretion, UP AR 525–17(S).

Chapter 9

The U.S. Army Intelligence Badge and Credential Program

9–1. General

a. This chapter establishes policy for the procurement, issue, use, control, and disposition of U.S. Army intelligence badges and credentials (B&C) and representative credentials. It applies to all active and RC MI units and to personnel authorized to use B&C or representative credentials.

b. B&C and representative credentials identify the bearer as a duly accredited special agent or representative of U.S. Army intelligence who is performing official intelligence duties.

9-2. Program functions

- a. The CG, PERSCOM and CG, ARPERCEN—
 - (1) Notifies the CG, INSCOM of the issuance or withdrawal of the SSI/MOS/civilian CI specialties.
 - (2) Furnishes copies of SSI/MOS orders on above personnel.
- b. The CG, INSCOM—
 - (1) Manages, and publishes administrative procedures for the USAI badge and credential and the badge trophy programs.
 - (2) Provides guidance to authorized users of USAI B&C and representative credentials.
 - (3) Operates the central repository for badges, credentials, credential forms, and associated items.
 - (4) Supervises the storage, control, accountability, issue, and disposition of badges, and credentials and credential forms: DA Forms 3363 and 3363-1, and DA Form 3363-A.
 - (5) Periodically inspects custodial accounts.
- c. Commanders—
 - (1) Appoint badge and credential custodians, sub-custodians, and their alternates to operate unit B&C accounts.
 - (2) Conduct semiannual inventories of all badges, credentials, and credential forms issued to the unit account or to unit personnel.
- d. The CG, U.S. Army Intelligence Center (USAIC)—
 - (1) Performs initial credentials processing for USAIC students attending CI courses 35E, 351B, and 97B.
 - (2) Informs INSCOM and PERSCOM or ARPERCEN when individuals are dropped from USAIC courses.
 - (3) Establishes procedures for RC intelligence training schools to inform INSCOM and ARPERCEN of SSI/MOS course completion.
 - (4) Issues B&C to Active Army graduating CI personnel.
- e. Persons issued B&C or representative credentials—
 - (1) Are responsible at all times for safeguarding their B&C or representative credentials unless properly relieved of this responsibility by the custodian, sub-custodian, or alternate.
 - (2) Are responsible at all times for the proper use of this documentation.
 - (3) Are required to become familiar with the provisions of this chapter.

9-3. Issue and retention of badges and credentials

B&C will be issued to the following personnel who are at least 21 years old and who possess a final TOP SECRET security clearance based on a Single Scope Background Investigation:

- a. Active Army personnel upon graduation from the 35E, 351B, or 97B course. These personnel retain their B&C as long as they are assigned/attached to the HQDA ODCSINT; INSCOM; 650th MI Group; USAIC; division, corps, and theater MACOM intelligence staff offices and supporting intelligence units; the On-Site Inspection Agency; the intelligence staff offices of unified and specified commands; the office of the Deputy Assistant Secretary of Defense (CI&SCM); and details to other service CI agencies or the FBI.
- b. U.S. Army civilian employees in job series GS-0132 assigned to CI units and duties, who have successfully completed a U.S. military CI officer/agent course, or non-DOD federal training that HQDA determines is equivalent.
- c. RC CI personnel upon activation: those called for duty individually will receive B&C through the Active Army unit custodian, and will turn them in at the end of that duty tour or the end of the mission requiring B&C, whichever is sooner. RC units will include B&C account activation and issue procedures in mobilization plans, and account inactivation and B&C return procedures during demobilization.
- d. Active Army B&C holders will return B&C to the central repository when leaving active duty or when reassigned to elements not listed in paragraph 9-3a. Civilians will return B&C upon outprocessing present employer (that is, when records transfer from one civilian personnel office to another or when leaving Army employment). In both cases, B&C must be returned through a B&C account custodian.
- e. Additional B&C policy is in AR 381-47(S).

9-4. Criteria for issue of representative credentials

Representative credentials are available for intelligence duties for which a badge is not required/authorized, for use while assigned to the requesting unit.

- a. Commanders may request representative credentials for personnel who conduct collection, liaison, or certain other intelligence duties, including—
 - (1) CI agent-trained personnel who are not yet 21 years old.
 - (2) MI personnel who hold SSI 35F or MOS 351C, or civilian GS-0132, and are assigned to HUMINT units.
 - (3) Foreign national employees of MI units assigned to investigative or liaison duties.
 - (4) Target exploitation (TAREX) personnel.

b. Commanders will endorse a detailed description of duties requiring the presentation of intelligence identification through command channels to INSCOM (IAOPS–HU/CI–OC).

c. Requests will include name, rank, SSI/MOS/civilian specialty, Social Security Number (SSN) or local national identification number, duty description, and verification of final TOP SECRET clearance for U.S. personnel or appropriate Limited Access Authorization for foreign national personnel. Requests are subject to the approval of the CG, INSCOM or his designated representative.

d. Additional policy on representative credentials is in AR 381–47(S).

9–5. Initial B&C issue by other than USAIC

a. RC schools will provide written notification to INSCOM and ARPERCEN of SSI/MOS course completion. Initial processing may be accomplished by RC units, or by an Active Army unit if the soldier is an Individual Mobilization Augmentee or Individual Ready Reserve. The following must be included: name, rank, SSI/MOS, SSN, verification of final TOP SECRET clearance, a copy of the SSI/MOS graduation certificate, and a copy of PERSCOM/ARPERCEN orders conferring the SSI/MOS in the request.

b. Units conduct initial processing of civilian personnel, if the civilian was not processed at USAIC. Name, grade, civilian specialty, SSN, verification of final TOP SECRET clearance, and a copy of the civilian’s graduation certificate must be included in the request.

c. Representative credentials will be processed and issued only upon the commander’s request, submitted and approved per paragraph 9–4.

9–6. Loss of B&C and representative credentials

Loss of B&C or representative credentials may be sufficient basis for disciplinary action and removal from such duties. Upon discovery of loss of a badge, credentials, or blank credential form, the accountable individual will notify his/her immediate superior and will conduct an immediate search of the suspected loss area. The individual’s unit will take the following actions:

a. Conduct an immediate recovery search.

b. Notify the B&C Controller by the fastest means available.

c. Investigate the circumstances UP AR 15–6.

d. As appropriate, notify local and national investigative agencies, including a full description of the badge and/or credentials.

e. Forward a summary of the investigative results through command channels to INSCOM. Include a request for relief from accountability and a statement of any disciplinary action taken, including action to remove the responsible individual from the CI program, as appropriate under military or civilian personnel regulations. Relief from accountability will be granted only upon satisfactory review of the investigative results and any corrective actions.

9–7. Misuse of B&C and representative credentials

a. The badge represents the enforcement aspect of CI; its use is, therefore, restricted to CI duties. B&C or representative credentials use for other than official intelligence duties is sufficient basis for disciplinary action and removal from such duties. The following is representative of misuse of the badge and credentials or representative credentials:

(1) Falsification, forgery, alteration of, or tampering with intelligence badges or credentials.

(2) Photographing or copying badges or credentials.

(3) Using a badge or credentials to represent oneself as a law enforcement official beyond the jurisdictional limits established by this regulation.

(4) Using a badge or credentials to gain access to information, facilities, or persons not required/authorized in the performance of official duties.

(5) Using a badge or credentials as identification when not on official intelligence duties; for example, in place of a DOD identification card to shop in the post exchange.

(6) Using a badge or credentials to perform functions not within the mission or authority of the element to which an individual is assigned or attached.

(7) Using a badge or credentials to perform functions which may be prohibited under the provisions of AR 381–10.

(8) Using a badge or credentials in an attempt to avoid civil citations, such as off-duty traffic or parking tickets.

b. Upon discovery of an alleged act of misuse, the unit commander—

(1) Will immediately initiate an investigation into the allegations in accordance with AR 15–6.

(2) May withdraw the B&C or representative credentials to custodian/sub-custodian control until the allegations are resolved.

(3) May impose administrative, non-judicial or judicial penalties as recommended by the investigation. Administrative penalties include removal from the CI program.

(4) Will provide through command channels to INSCOM a summary of the investigative results. Include, as

appropriate, a statement of any disciplinary or administrative action and/or action to remove the individual from the CI program.

9–8. Central badge and credentials repository

a. The B&C Controller holds badges and credentials of authorized personnel whose current duties do not require their use.

b. The central repository maintains B&C of personnel honorably separated or retired from active duty or USAI civilian employment for two years after turn-in. The Controller then destroys credentials and holds the badge another year for issuance under the trophy program, after which the badge is returned to the general inventory.

c. RC unit commanders will regularly provide a roster to the B&C Controller of all assigned personnel who hold a CI SSI/MOS, regardless of whether they are assigned to a CI SSI/MOS duty position. Providing the roster ensures B&C are manufactured and held at the repository until a requirement for their issuance is forwarded.

d. Personnel not on CI duties may choose to return B&C, through an account custodian, to the central repository for safekeeping.

9–9. The Counterintelligence Badge Trophy Program

a. INSCOM will provide an opportunity for personnel who have served in Army counterintelligence to receive a symbol of that service upon retirement or after final honorable separation from Army service or employment.

b. To be eligible for the badge trophy, the applicant must have—

- (1) Qualified as a CI special agent as prescribed by the regulations in effect at the time the applicant was trained.
- (2) Not had the CI specialty withdrawn for cause.
- (3) Received an honorable discharge, be retired, or resigned under favorable conditions.
- (4) Been released/retired from the Reserve Components.

c. The trophy is provided at the individual's own expense.

Chapter 10 Intelligence Polygraphs

10–1. General

Army intelligence investigations and operations depend on relevant evidence and dependable information, secured through skillful investigations and interrogations. The polygraph examination is an aid to support other investigative means, and will not be used as the only investigative tool. Use of the polygraph examination in conjunction with Army intelligence activities must conform to the policy in this chapter, app E, and AR 195–6.

10–2. Use of intelligence polygraph examinations

Intelligence polygraph examinations are authorized for the following:

a. CI investigations. Civilian, military, contractor and other personnel may be requested to submit to a polygraph examination in connection with a CI investigation, provided that—

- (1) Investigation by other means has been as thorough as circumstances permit;
- (2) Information development via a polygraph examination is essential to the investigation;
- (3) The potential examinee has been interviewed, and there is reasonable belief that he has knowledge of or was involved in the matter under investigation.

b. Foreign intelligence and CI operations. These operations determine the suitability, reliability, or credibility of agents, sources, or operatives.

c. Personnel security investigations. These polygraphs are conducted to—

- (1) Verify background information when it cannot be verified by other means;
- (2) Resolve credible derogatory information, when this information causes substantial doubt as to whether access or continued access to classified information is clearly consistent with the interests of national security, and the derogatory information cannot be resolved in any other manner.
- (3) Ensure that foreign national access to sensitive or classified information is clearly consistent with the interests of national security. Such examinations should not be authorized if they would violate the laws of the host country or any security agreement between the United States and the host country.

d. Access to sensitive compartmented information (SCI). When operational exigencies require a person's immediate access to SCI before completion of a PSI, a polygraph may be conducted provided that—

- (1) Appropriate exceptions to SCI policy are approved;
- (2) A PSI has been initiated; and
- (3) The examination scope is limited to the topics used in a CI scope polygraph examination.

e. Exculpation. The subject of a personnel security or CI investigation requests a polygraph, and the examination is considered essential to a just and equitable resolution of the matters under investigation. The subject should support the request in writing, citing specific details countering the investigative findings.

f. Non-DOD polygraph support. Non-DOD agencies may request intelligence polygraph support through DOD. If DOD approves, the appropriate service polygraph component will be tasked to provide that support.

g. CI scope polygraph (CSP) examinations. (See app E) CSP may be used to determine the initial and continued eligibility of military, civilian, and contractor personnel for—

- (1) Access to specifically designated SAPs.
- (2) Access to specifically designated TOP SECRET information.
- (3) Employment/assignment to DIA in designated critical intelligence positions.
- (4) Access, employment, assignment or detail to the National Security Agency (NSA); access to sensitive cryptologic information; or access to NSA spaces where sensitive cryptologic information is produced, processed, or stored. The examination must be favorably resolved.
- (5) Access to non-NSA spaces where sensitive cryptographic information is produced, processed, or stored.
- (6) Employment by, assignment or detail to DOD activities concerning collection of national foreign intelligence through special reconnaissance programs.
- (7) Assignment or detail to CIA.

10-3. Selection, training, and certification of intelligence polygraphers

CI special agents may apply for polygraph training in accordance with policy in AR 195-6.

10-4. Requesting intelligence polygraph support

Submit requests for intelligence polygraph support to INSCOM (IAOPS-CI-TG), in accordance with procedures in AR 195-6.

Appendix A References

Section I Required Publications

AR 1-40

Clearance Requirements and Procedures for Official Temporary Duty Travel Outside the Continental United States. (Cited in para 8-10.)

AR 27-40

Litigation. (Cited in para 8-14.)

AR 190-6

Obtaining Information from Financial Institutions. (Cited in para 8-15.)

AR 190-14

Carrying of Firearms and Use of Force for Law Enforcement and Security Duties. (Cited in para 8-9a.)

AR 190-22

Searches, Seizures and Disposition of Property. (Cited in paras 8-13a, 8-13b.)

AR 190-27

Army Participation in National Crime Information Center. (Cited in para 4-8.)

AR 195-2

Criminal Investigation Activities. (Cited in paras 2-8f, 2-11k.)

AR 195-6

Department of the Army Polygraph Activities. (Cited in paras 2-5a, 4-1 b, 5-7a(2), 10-1, 10-3, 10-4, E-9c(2).)

AR 340-21

The Army Privacy Program. (Cited in para 8-15a, E-22c.)

AR 380-5

Department of the Army Information Security Program. (Cited in paras 4-2b(11), 8-3c, B-5a, B-6c, D-4a, E-23(c)(7).)

AR 380-13

Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations. (Cited in para 5-12a.)

AR 380-53

Communications Security Monitoring. (Cited in paras 5-15a.)

AR 381-10

U.S. Army Intelligence Activities. (Cited in paras 1-5b(5), 2-4g, 2-17, 4-1b, 4-2 g, 4-8d, 5-11a, 5-18b, 9-8a(7).)

AR 381-12

Subversion and Espionage Directed Against the U.S. Army (SAEDA). (Cited in paras 2-11e, 2-11f, 2-13, 3-3 d, 4-1b, 4-4a.)

AR 381-45

Investigative Records Repository (IRR). (Cited in para 3-2f.)

AR 500-51

Support to Civilian Law Enforcement. (Cited in para 8-12c.)

AR 600-40

Apprehension, Restraint, and Release to Civil Authorities. (Cited in para 8-12a.)

AR 670-1

Wear and Appearance of Army Uniforms and Insignia. (Cited in para 8-5b.)

AR 700-84

Issue and Sale of Personnel Clothing. (Cited in para 8-5e.)

FM 34-60

Counterintelligence. (Cited in para 5-16b.)

MCM

Manual for Courts-Martial. (Cited in paras 8-13a.)

18 USC 801-940

Uniform Code of Military Justice (Contained in MCM). (Cited in paras 1-4e, 8-10, 8-11a.)

Section II

Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this publication.

Agreement of 5 April, 1979

Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation, 5 April, 1979.

AR 10-5

Organization and Functions, Headquarters, Department of the Army.

AR 10-87

Organization and Functions, Major Army Commands in the Continental United States.

AR 15-6

Procedures for Investigative Officers and Boards of Officers Conducting Investigations.

AR 25-55

The Army Freedom of Information Act Program.

AR 27-10

Military Justice.

AR 40-63

Ophthalmic Services.

AR 70-1

Systems Acquisition Policy.

AR 71-9

Materiel Objectives and Requirements.

AR 140-192

Organization, Training, Assignment, and Retention Criteria for Military Intelligence, Signals Intelligence, Electronic Warfare, and Signals Security Units (Reserve Components).

AR 190-9

Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies.

AR 190-24

Armed Forces Disciplinary Control Boards and Off-Installation Military Enforcement.

AR 190-28

Use of Force by Personnel Engaged in Law Enforcement and Security Duties.

AR 190–30

Law Enforcement Investigative Activities. (Military Police Investigations)

AR 190–40

Serious Incident Report.

AR 190–47

The U.S. Army Correctional System.

AR 195–5

Evidence Procedures.

AR 210–11

Installation—Billeting Operations.

AR 380–19

Information Systems Security.

AR 380–67

Personnel Security Program.

AR 380–381 (S)

Special Access Programs (SAPs) (U).

AR 381–11

Threat Support to U.S. Army Force, Combat, and Material Development.

AR 381–14(S)

Technical Surveillance Countermeasures (TSCM) (U).

AR 381–19

Dissemination and Production Support.

AR 381–47 (S/NF)

U.S. Army Offensive Counterespionage Activities (U).

AR 381–100 (S)

U.S. Army Human Intelligence Collection Programs (U).

AR 381–102 (S)

U.S. Army Cover Support Program (U).

AR 381–141 (C)

Intelligence Contingency Funds (U).

AR 381–143 (C)

Military Intelligence Logistics Policies and Procedures (U).

AR 381–171 (S)

International Intelligence Agreements (U).

AR 530–1

Operations Security.

AR 525–13

The Army Combatting Terrorism Program.

AR 600–200

Enlisted Personnel Management System.

AR 604-10
Military Personnel Security Program.

AR 606-15
Preparation of Fingerprint Record.

AR 611-101
Commissioned Officer Classification System.

AR 614-115 (C)
Military Intelligence Excepted Career Program (Great Skill Program) (U).

AR 614-200
Selection of Enlisted Soldiers for Training and Assignment.

AR 630-10
Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings.

AR 690-950-19-1 (S)
Military Intelligence Civilian Excepted Career Program (U).

Attorney General Guidelines for FBI Supervision or Conduct of Espionage Investigations of U.S. Diplomatic Missions Personnel Abroad.

28 CFR 60
Code of Federal Regulations, Authority of Federal Law Enforcement Officers to Request the Issuance of a Search Warrant.

DCID 1/7
Control of Dissemination of Intelligence Information.

DCID 1/14
Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information.

DCID 5/1 (S)
Espionage and Counterintelligence Activities Abroad (U).

DIS 20-1-M
Manual for Personnel Security Investigations.

DOD 4640.6
Communications Security Monitoring.

DOD 5200.27
Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense.

DOD 5240.2
DOD Counterintelligence.

DOD 5240.4
Reporting of Counterintelligence and Criminal Violations.

DOD 5100.78
United States Port Security Program.

DOD 5210.48
DOD Polygraph Program.

DOD 5210.48-R

Department of Defense Polygraph Program.

DOD 5240.5

DOD Technical Surveillance Countermeasures (TSCM) Survey Program.

DOD 5240.10

DOD Counterintelligence Support to Unified and Specified Commands.

EO 12333

United States Intelligence Activities.

FM 19-20

Military Police Criminal Investigations.

FM 19-30

Physical Security.

FM 27-10

The Law of Land Warfare.

FM 34-5 (S/NF)

Human Intelligence and Related Counterintelligence Operations (U).

Joint Pub 1-02

DOD Dictionary of Military and Associated Terms.

Joint Pub 2-01.2 (S/NF)

Doctrine and Tactics, Techniques and Procedures for Counterintelligence Support to Joint Operations. (U)

5 USC 303

United States Code, oaths to witnesses.

5 USC 552

United States Code, access to federal agency information.

10 USC 807-809

United States Code, armed forces statutes covering apprehension authority.

12 USC 3401-3419

United States Code, access to financial records by government authorities.

15 USC 1681f

United States Code, consumer reporting agencies' release of information to government agencies.

18 USC 701

United States Code, criminal statute covering official badges, identification cards, and other insignia.

18 USC 792-798

United States Code, criminal statutes covering espionage and deliberate disclosure of classified defense information.

18 USC 912

United States Code, criminal statute covering impersonation of an officer or employee of the United States.

18 USC 2151-2156

United States Code, criminal statutes covering sabotage.

18 USC 2381

United States Code, criminal statute covering treason.

18 USC 2382–2385

United States Code, criminal statutes covering sedition.

18 USC 2387–2388

United States Code, criminal statutes covering subversion.

28 USC 535

United States Code, investigative agencies.

50 USC 401

United States Code, The National Security Act of 1947.

50 USC 421

United States Code, The Intelligence Identities Protection Act.

50 USC 1801

United States Code, The Foreign Intelligence Surveillance Act of 1978.

Section III

Prescribed Forms

DA Form 3363

U.S. Army Intelligence Credential. (Prescribed in para 9–2a.)

DA Form 3363–1

U.S. Army Intelligence Credential. (Prescribed in para 9–2a.)

DA Form 3363–A

U.S. Army Intelligence Credential (Representative). (Prescribed in para 9–2a.)

Section IV

Referenced Forms

This section contains no entries.

Appendix B Security Considerations

B-1. Purpose

This appendix provides general policy on classification and dissemination of information pertaining to CI units, personnel, and activities.

B-2. Classification guides

All CI units will use the classification guidance provided in AR 381-14(S) and AR 381-47(S/NF), as applicable. When the classification of a specific item, activity, or situation is uncertain despite the guidance, forward a request for classification determination to HQDA (DAMI-CIC). Pending a final determination, safeguard the information at a minimum of CONFIDENTIAL.

B-3. Publicity

Do not discuss intelligence matters publicly. Conduct no interviews of CI personnel or release for publication any information relative to U.S. Army CI investigations (open or closed), operations, collection, production, personnel, or units without prior approval of HQDA (DAMI-CI).

B-4. Evaluation reports

Classify evaluation reports when they include any of the following:

- a.* A description of classified duties performed.
- b.* Statements of operational proficiency if classified duties are discussed.
- c.* The rated individual's true status is classified.

B-5. Debriefing

a. When the need-to-know requirements of personnel assigned to CI duties or activities cease, the unit commander will have them orally debriefed in accordance with AR 380-5. Conduct this debriefing before the person is retired/released from active duty or civilian employment, on the withdrawal of one of the specialties listed in paragraph 8-1*b*, or at any time the unit commander deems appropriate.

b. This CI specific debriefing is not required for personnel transferring from one assignment to another when the new assignment will be to similar CI duties. Do not use this debriefing in lieu of normal security out-processing requirements.

B-6. Screening personnel records

Losing units will—

- a.* Screen records of persons with a specialty listed in paragraph 8-1*b*, when any of the following occurs:
 - (1) Release, discharge or retirement from the service.
 - (2) Resignation, termination or retirement of civilian employee.
 - (3) Reassigned from CI duties to non-CI duties in another unit.
- b.* Declassify records when appropriate.
- c.* In accordance with AR 25-400-2, AR 380-5, AR 381-47 and this regulation, withdraw and retire or destroy information that should remain classified.

Appendix C Selected Counterintelligence Addresses

C-1. HQDA, Office of the Deputy Chief of Staff for Intelligence, Directorate of Counterintelligence and Security Countermeasures:

Mailing address: HQDA
ATTN: DAMI-CI
Washington, DC 20310-1050

GENSER address: DA WASH DC//DAMI-CI//
SSO address: SSO DA//DAMI-CI//
Sub-office symbols: DAMI-CIC (Counterintelligence Division), DAMI-CIS (Security Countermeasures Division), DAMI-CIT (Technology Transfer Division)

C-2. U.S. Army Intelligence and Security Command, Assistant Deputy Chief of Staff for Operations-Counterintelligence:

Mailing address: Commander
U.S. Army Intelligence and Security Command
ATTN: IAOPS-HU/CI
Fort Belvoir, VA 22060-5370

GENSER address: CDRINSCOM FT BELVOIR VA//IAOPS-HU/CI//
SSO address: SSO INSCOM//IAOPS-HU/CI//
Sub-office symbols: IAOPS-HU/CI-CI-O (Operations Division), IAOPS-HU/CI-CI-T (Technical Division), IAOPS-HU/CI-CI-TG (Polygraph Division)

C-3. Commander, U.S. Army Intelligence and Threat Analysis Center, Counterintelligence and Terrorism Division:

Mailing address: Commander
US Army Intelligence and Threat Analysis Center
ATTN: IAITAC-RK
Bldg 213, Washington Navy Yard
Washington, DC 20374-2136

GENSER address: CDRUSAITAC PENTAGON WASH DC//IAITC-RK//
SSO address: SSO ITAC//IAITC-RK//

C-4. Army Central Control Office:

Mailing address: Chief
Army Central Control Office
ATTN: DAMI-CIC-CCO
Fort Meade, MD 20755-5975

GENSER address: ACCO FT MEADE MD//DAMI-CIC-CCO//
SSO address: SSO MEADE//DAMI-CIC-CCO//

C-5. Antiterrorism Operations and Intelligence Cell:

Mailing address: HQDA
ATTN: DAMO-ODL-CBT
Washington, DC 20310-0440

GENSER address: DA WASH DC//DAMO-ODL-CBT//
SSO address: SSO DA//DAMO-ODL-CBT//

Appendix D Courtesy Letter Program

D-1. General

The courtesy letter program is used to determine whether CI personnel are conducting PSI in an ethical and professional manner. Information gathered by this program identifies potential investigative problems or shortcomings and provides training and counseling to the investigator. It is used to evaluate an investigator's competence and to reinforce the importance of integrity and accurate reporting.

D-2. Program functions

- a.* The DIS is responsible for the overall DOD PSI program and the DIS Courtesy Letter Program.
- b.* ODCSINT, HQDA is responsible for Army policy regarding the Courtesy Letter Program.
- c.* Commanders of units who perform PSI are responsible for the conduct and control of the courtesy letter program within their areas of jurisdiction.

D-3. Procedures

Commanders will establish procedures to identify those personnel on whom courtesy letter coverage is required and to what extent. Those procedures will include—

- a.* Random selection of recently completed PSI reports and agent's notes. Leads conducted telephonically must be clearly annotated.
- b.* A minimum of two monthly letters for all personnel in their first year of performing PSI.
- c.* A minimum of one quarterly letter for all other personnel.

D-4. Local inquiries

a. Local inquiries are conducted to resolve minor matters and to determine if corrective action, such as counseling or remedial training, is necessary. A local inquiry should be initiated when one of the following situations occurs:

- (1) A courtesy letter questionnaire discloses that an interview was conducted by telephone, and this was neither authorized by DIS 20-1-M nor justified in the PSI report or agent's notes.
 - (2) A courtesy letter questionnaire indicates that the investigator failed to meet one or more of the interview standards outlined in paragraph D-6.
 - (3) A courtesy letter questionnaire discloses that the interview results reported by an investigator are inaccurate.
 - (4) Two or more courtesy letter questionnaires pertaining to a particular investigator are returned "addressee unknown" within a month.
- b.* Supervisory investigators will conduct local inquiries. These should be limited to a reinterview of the addressee—
- (1) Under the pretext of a courtesy contact, or
 - (2) If no response was received, to confirm that the addressee actually resided or worked at the reported address at the time the investigative lead was accomplished.
- c.* Because this is an administrative procedure, do not obtain sworn statements.
- d.* File favorably resolved inquiry results as stated in paragraph D-5.
- e.* If the results mandate further administrative or investigative action, or indicate an investigator has falsely reported having conducted a PSI lead, comply with the appropriate provisions in AR 15-6 and AR 381-10, procedure 15.

D-5. Disposition

- a.* Forward favorable questionnaires to the investigator.
- b.* When a questionnaire is not answered or is returned by postal authorities as "addressee unknown," retain it for one year with the report or agent's notes, or until inquiries or sufficient positive questionnaires favorably resolve the matter, whichever is sooner.
- c.* Destroy a questionnaire that contains critical comments, along with the report or agent's notes after one year or when any subsequent actions have been completed. If a questionnaire indicates that an agent falsely reported having interviewed an addressee, or committed some other major violation, retain it in the AR 15-6 files.

D-6. Courtesy letter format

Prepare courtesy letters on letterhead, in non-military letter style. The letter should include the date of the interview, the name of the investigator, who should give a brief reason for the questionnaire, thank the addressee for his/her support, and enclose a postage-paid addressed envelope for returning the questionnaire. The questionnaire, attached as an enclosure, will solicit input on—

- a.* Proper introduction and presentation of credentials by the investigator (personal interview) or proper introduction of the investigator (telephonic interview).
- b.* Whether the investigator clearly articulated the reason for the interview.
- c.* Whether the investigator asked pertinent, clear, and direct questions.
- d.* Whether questions were specific and detailed regarding the subject's character, integrity, habits, and reputation.
- e.* Whether the addressee was asked if he/she recommended the subject for a position of trust with the U.S. Government.
- f.* The investigator's manner.
- g.* The investigator's appearance (personal interview).
- h.* Additional comments or recommendations by the addressee.
- i.* Whether the addressee wishes to speak with a supervisory investigator and the addressee's daytime phone number if an appointment is desired.

Appendix E

Counterintelligence Scope Polygraph Program

Section I

General

E-1. Summary

This appendix implements DOD policies, procedures and guidance, and establishes Army policy and procedures for the Counterintelligence Scope Polygraph (CSP) Program.

E-2. Purpose

The CSP examination is a Congressionally authorized CI investigative screening technique to deter and detect espionage and sabotage. It is a component of a comprehensive and continuing CI and Security Countermeasures Program. USAI uses CSP examination results to determine if a person is or has been involved in espionage or sabotage.

E-3. Centralized program management

To attain uniform implementation of a CSP program throughout DOD, program management and responsibility is centralized. The HQDA DCSINT, the Assistant DCSINTs, or the Chief, CI and Security Countermeasures Directorate, may approve waivers or exceptions to Army CSP policies and procedures. Requests for exceptions or waivers are sent through command channels to HQDA (DAMI-CI).

E-4. Where CSP are authorized

CSP examinations are authorized for personnel whose official duties involve access to specific categories of classified information. All personnel requested to take a CSP examination must be assigned, or be scheduled for assignment or detail, to a position involving duties that are authorized polygraph support.

a. SAP access. A CSP examination is authorized to assist in determining initial and continued eligibility for access to SAP information (AR 380-381).

(1) Army personnel and defense contractors whose duties involve access to information within Secretary of the Army (SA) designated and DOD-approved SAPs may be subject to random selection for a CSP examination.

(2) USAI may conduct a CSP examination of Army or non-Army personnel based on SAP access if authorized by DOD, or when requested by a DOD component that does not have a polygraph examination capability.

b. TOP SECRET access. Army personnel and defense contractors whose duties involve access to DOD-specified categories of TOP SECRET (TS) information may be subject to CSP examinations.

c. Assignment or detail to NSA. USAI polygraph examiners conduct CSP examinations prior to the individual's assignment or detail to NSA. The Director, NSA (DIRNSA), is the final determining authority for approving or denying assignment or detail when a deception indicated (DI) or inconclusive (INC) CSP examination occurs, or when there are admissions in a no deception indicated (NDI) examination.

d. Other related polygraph examinations. DOD Directive 5205.8 and AR 380-40 require CSP examinations in support of the Cryptographic Access Program. Polygraph examinations may be conducted of Army personnel assigned or detailed to the CIA, certain DIA critical positions, or assigned or detailed to a DOD element responsible for collection of foreign intelligence through special reconnaissance programs.

e. Numerical ceiling. Public law restricts SAP, TS and DIA CSP examinations to an annual numerical ceiling. NSA, CIA, cryptographic access programs, and reconnaissance CSP examinations are not subject to a ceiling.

E-5. CSP Program functions

a. Secretary of the Army. Only the SA may make an unfavorable personnel security determination based solely on CSP examination chart results of DI. This authority is not further delegated.

b. The Director, Technology Management Office (TMO), Office of the Chief of Staff, HQDA. The Director, TMO ensures that any individual with Army SAP access who refuses to take a CSP examination based on SAP access, is denied further access to all SAP information under Army control. The TMO will notify DOD of the individual's refusal to take a SAP CSP examination.

c. The DCSINT. The DCSINT—

(1) Exercises Army general staff responsibility for the CSP program.

(2) Develops Army CSP policies and general procedures.

(3) Processes waivers or exceptions to DOD CSP policies and approves waivers or exceptions to Army CSP policies.

(4) Processes requests for a SA decision regarding an unfavorable personnel security determination subsequent to a CI investigation of DI CSP examination.

(5) Upon referral from INSCOM and in coordination with the AGC and TJAG, determines if an examinee's spontaneous comments to CSP technical questions are an admission to a specific, significant criminal offense.

d. The DCSPER. The DCSPER establishes personnel management procedures to ensure that—

(1) Applicants for employment or assignment to positions whose duties are subject to a CSP examination are not placed in such a position, if they refuse to take a CSP examination.

(2) Army military personnel and civilian employees who refuse to take a CSP examination are retained in a position of equal pay and grade that is not subject to a CSP examination.

(3) A refusal to take a CSP examination is not recorded in the individual's personnel records and is not permitted to influence the individual's official evaluation report or eligibility for awards or promotion.

(4) Personnel are not assigned or detailed to NSA when he or she refuses to take the NSA CSP examination, or does not favorably complete the NSA CSP examination.

e. CG, INSCOM. The CG, INSCOM will—

(1) Manage and administer (for the DCSINT) the CSP program. INSCOM has technical authority, direction, quality control, and oversight of all CSP examinations administered by USAI polygraph examiners.

(2) Plan, program, and budget for the conduct of CSP examinations.

(3) Ensure that SAP and TS CSP examinations do not exceed the DOD-assigned annual allocation.

(4) Ensure that CSP examination refusals and CSP examination results of No Opinion (NO), DI, or INC are processed consistent with DOD Directive 5210.48, and DOD5210-48-R, and this appendix.

(5) Maintain a central registry with the identities and results of CSP examinations.

(6) Annotate the Defense Clearance and Investigations Index to indicate the conduct of USAI CSP examinations.

(7) Advise program managers, commanders, and HQDA staff heads that an individual has met his or her obligation to take a CSP examination.

(8) Process appropriate waivers or exceptions to the DIRNSA, for Army personnel assignments or details to NSA based on other than favorably completed CSP examinations.

(9) Determine if an examinee's spontaneous comments to CSP technical questions may be an admission to a specific, significant criminal offense.

(10) Not assign or detail an INSCOM individual to NSA when he or she refuses to take the NSA CSP examination, or does not favorably complete the NSA CSP examination.

f. HQDA agency heads and Army MACOM commanders with personnel who are subject to CSP examinations. These officials—

(1) Schedule required CSP examinations, in coordination with INSCOM.

(2) Ensure that Army and defense contractor personnel under their purview attend scheduled CSP examinations.

(3) Deny further access to SAP, TS, or cryptographic access program information when an individual refuses to take a scheduled CSP examination.

(4) Comply with the provisions of paragraph E-6.

E-6. CSP controls and prohibitions

The following controls govern the CSP program, to protect the rights and privacy of an individual before, during, and after the CSP examination.

a. CSP examinations. CSP examinations are voluntary. Individuals will not be penalized because they refuse to take a CSP examination. Refusal to take a CSP examination must be properly balanced with the DOD's security interests. No adverse action (AR 380-67) will be based solely on the fact of a refusal or because the person terminated a CSP examination. In the case of a CSP refusal, however, a person may be transferred to a position of equal pay and status where the duties do not involve access subject to a CSP examination.

b. Unfavorable personnel security determinations. An investigation will be conducted following a CSP examination with DI results. If the investigation develops no derogatory information upon which an unfavorable personnel security determination (AR 380-67) can be based independently, such a determination will not be made, unless approved by an authority listed in DOD 5210.48-R. This decision must be based on the determination authority's written finding that information is of such extreme sensitivity that access under the circumstances is clearly not consistent with the interests of national security.

c. Prohibited actions. Prohibited unfavorable administrative actions (AR 380-67), based only on CSP examination charts or general information that a person did not favorably complete a CSP examination, include but are not limited to—

(1) Denial or withdrawal of access to national security information. This includes temporarily suspending a person's access to SCI, SAP, or cryptographic program information, or access to other categories of classified information.

(2) Denial, suspension, or revocation of a security clearance.

(3) Reassigning a person to a position of lesser sensitivity or to a non-sensitive position.

(4) "Flagging" a military member's personal file to defer favorable actions.

d. Eligibility for other positions. Within the Army, consent to a CSP examination may be a condition of continued

access, but it should not be considered a condition of continued employment. A person's employment or military service will not be terminated based on termination of or a refusal to undergo a CSP examination. Commanders, chiefs, and agency heads, in coordination with their supporting personnel management officials, will ensure that individuals who refuse to take a CSP examination are retained in a position of equal grade and pay involving duties that are not subject to a CSP examination. This may require that they arrange employment for the individual at another DOD component.

E-7. CSP topics and questions

a. Topics. The CSP examination will cover no "lifestyle" issues such as the use of drugs or alcohol, morals, financial matters, or arrests. The CSP examination is limited to the following CI topics:

(1) Involvement in espionage against the United States: committing, assisting others, and knowledge of espionage activity.

(2) Involvement in sabotage against the United States: committing, assisting others, and knowledge of sabotage activity.

(3) Unauthorized disclosure of classified information: the disclosure of classified information or material through any means to any unauthorized person.

(4) Unauthorized foreign contacts: unauthorized, clandestine or secret contact with a non-U.S. person or someone (U.S. or non-U.S.) who represents a foreign government, power, group or organization or firm.

b. CI questions. Only the CI topics listed above will be used in CSP examination questions. Any substantive modification to these topics must be approved by the Deputy Assistant Secretary of Defense (CI & Security Countermeasures) or Director, CI, before use. The prior approval requirement does not apply when modifying or clarifying the phrasing of an approved question topic, as long as the topic substance remains unchanged.

c. Technical questions. Technical questions are the baseline against which responses relevant to the CI topics are evaluated. Technical questions will be constructed to avoid embarrassing, degrading, or unnecessarily intrusive topics. Technical questions probing a person's religious and racial beliefs and affiliations, political beliefs and affiliations of a lawful nature, and opinions regarding the constitutionality of legislative policies are prohibited unless specifically related to the relevant CI topics. All technical questions must be reviewed with the examinee before being asked during the in-test phase. If it appears that a technical question might result in the admission of a crime, another question will be selected.

E-8. CSP examination conclusions

Based upon an analysis of relevant CSP charts, a polygraph examiner may render one of four possible conclusions concerning the CSP examination:

a. No Opinion (NO). Zero or one charts are conducted concerning the relevant CI topics.

b. Inconclusive (INC). Test results provide insufficient information upon which to make a determination of NDI or DI.

c. No Deception Indicated (NDI). Responses are judged by the polygraph examiner to be truthful.

d. Deception Indicated (DI). Responses are judged by the polygraph examiner to be untruthful.

E-9. Reporting admissions

The CSP examination is not intended to detect administrative security violations or to identify every foreign contact. It will not be used to elicit admissions to criminal activities other than espionage or sabotage. However, information will be reported if the individual makes a spontaneous admission to a serious, specific criminal offense.

a. Reportable admissions.

(1) Committing, assisting others, and knowledge of espionage or sabotage against the United States.

(2) Significant disclosures of classified information or material to an unauthorized person.

(3) Unauthorized foreign contacts that involve CI issues. Casual contact with non-U.S. citizens and authorized contact with foreign representatives are not reported.

b. Use of admissions. Admissions reported in a Polygraph Examination Report (PER) and sworn statements obtained by polygraph examiners are investigative leads and may be used in CI investigations to confirm or refute CI issues. The admissions also may be used in unfavorable personnel actions and personnel security determinations, when they constitute credible derogatory information (AR 380-67).

c. Spontaneous admissions to technical CSP examination questions. As a general rule, polygraph examiners will not document the nature and content of an examinee's comments to a technical question, unless there are spontaneous admissions of a specific, significant criminal offense. Spontaneous admissions may occur at any time during the CSP examination process.

(1) Before continuing the examination, the examiner will consult with his supervisor and supporting SJA for guidance.

(2) If an examinee admits to committing a specific, significant criminal offense in response to a technical question, the information will be recorded in the PER and disseminated per AR 195-6.

(3) If the polygraph examiner or supervisor is unable to determine if the examinee's comments constitute a specific, significant criminal offense after consultation with the supporting SJA, the information will be referred to INSCOM. If INSCOM is unable to make a determination, the information will be referred to HQDA (DAMI-CI).

d. Other information. Other derogatory information derived from admissions to CI topics should be resolved to serve the best interests of both the individual and the Army.

E-10. CSP examination refusals and termination

a. Refusal types.

(1) Position applicant refusals are individuals who apply for, or are offered employment, assignment, or detail to positions involving duties that require or subject them to a CSP examination. If they do not consent to take a CSP examination, they will not be selected or assigned to a position subject to a CSP examination.

(2) Position incumbent refusals are individuals assigned in positions whose duties require a polygraph examination as a condition of access, employment, assignment, or detail. They occupy the position, subsequently are requested to take a CSP examination, but refuse. Incumbent refusals may be denied further access, assignment, or detail to such positions. However, with the exception of NSA, the DOD component concerned will ensure that the individual is retained in another position of equal grade and pay that does not require a CSP examination, or arrange like employment at another DOD component.

b. Other circumstances that constitute a refusal.

(1) An examinee terminates a CSP examination prior to the collection of at least one series of polygraph charts.

(2) A person is contacted to schedule a CSP examination, then deliberately obtains an access debrief to evade the CSP examination. However, if the proponent of the information or program has scheduled a debriefing prior to notification of a scheduled CSP examination, the person will not be considered a refusal or requested to take a CSP examination.

(3) INSCOM will notify the program manager or commander following a person's second failure to attend a scheduled CSP examination and request assistance. Should the individual fail to attend the third scheduled CSP examination, he will be processed as a refusal.

c. Refusal interviews. A person who refuses to take a CSP examination will be requested to undergo a non-acusatory interview with a polygraph examiner, and asked to submit a declination statement citing the reasons for refusing. If the individual declines the interview, or declines to provide a written statement, the INSCOM polygraph examiner will prepare a memorandum that summarizes the declination circumstances. The declination statement or memorandum will be forwarded to the ACCO.

d. Other terminations. The examinee may terminate a CSP examination at any time. The examiner bases his conclusion on the analysis of CSP examination charts obtained prior to the termination. The individual's reasons for termination will be included in the PER. Do not report the reasons for the termination to the individual's organization or the CSP requester.

E-11. Recording and monitoring

a. Recording CSP examinations. All CSP examinations will be audio or video recorded from beginning to end. A recording of routine examinations will be retained for 90 days following the date of the last examination, then erased. When the conduct or results of the examination might reasonably be expected to lead to grievances, administrative or judicial action, recordings will be retained until completion of the action. If no action is initiated, the recording will be erased 180 days after quality control review.

b. Monitoring CSP examinations. Only the examinee and the polygraph examiner(s) will be in the examination room during the in-test phase. Polygraph examiner, supervisory, and quality control personnel may monitor an examiner's conduct of a CSP examination by visual or audio means. Visual means may include an observation mirror or remote, real-time video. Examinee counsel or a union representative may observe the examination from outside the examination room by audio or visual means. INSCOM may authorize exceptions on a case-by-case basis.

E-12. Medical suitability for CSP examinations

a. The examiner may refuse to conduct a CSP examination, or discontinue testing, when the examiner doubts that the examinee is physically or mentally fit for testing. Examiners will not make psychiatric or physical diagnosis. The examination will be postponed until appropriate medical, psychological, or technical authorities have determined the individual is fit for testing. The examination will not be given when, in the opinion of the examiner, a person cannot respond due to any of the conditions listed below:

- (1) Mental or physical fatigue.
- (2) Mental disorder.
- (3) Extreme emotional stress, intoxication, narcotics addiction, or excessive use of depressants, stimulants, tranquilizers, or hallucinogens.
- (4) Physical discomfort or disability.

b. When there is a question regarding a person's medical suitability for testing, INSCOM will forward information

on the medical condition to the CSP requester. The CSP requester will arrange to have a military doctor or contract physician evaluate the individual's medical records, and the individual if necessary, to determine whether or not the person is medically fit to undergo a CSP examination. The individual, and the individual's private physician, may submit relevant medical information for consideration by the military doctor or contract physician. Medical evaluation results will be returned to INSCOM.

c. Individuals who are medically cleared will be requested to take a CSP examination. Individuals not medically cleared will be authorized access to SAP, cryptographic, or designated TS information without the examination. For personnel scheduled for assignment or detail to NSA, INSCOM will determine if a CSP examination waiver should be submitted to the DIRNSA.

E-13. Other agency CSP examinations

CSP examinations conducted by other federal agencies covering the CI topics listed in paragraph E-7 may be accepted in lieu of an Army-administered CSP examination.

E-14. CSP examiners

CSP examinations will be conducted by certified intelligence polygraphers, or by intern examiners under supervision of a certified examiner.

Section II

Conduct of a CSP examination

E-15. Notification

The person being contacted for a CSP examination will be given timely notification of the date, time, and place of the examination. During this initial contact, verify that the person's current or pending duties are in a position subject to a CSP examination. If there is any question regarding the person's duties, position, or access, resolve it before scheduling the CSP examination.

E-16. Prebrief

Each examinee will receive a prebrief before the CSP is conducted. This initial briefing will include the reasons for the CSP program, the CI topic areas, and an overview of the polygraph process. The briefing should be done at least 24 hours before the examination, and may be a videotape or personal briefing. If that is not possible, provide at the minimum a written prebrief before the examination.

E-17. Pre-test interview

The pre-test interview of a CSP examinee will—

- a. Emphasize that the individual is not suspected or accused of any crime or wrongdoing.
- b. Verify that the individual's current or pending duties are subject to a CSP examination.
- c. Advise the individual if the polygraph examination area contains a viewing window or mirror, camera, microphone, audio or video recorder, or any other device to monitor or record the examination.
- d. Advise the individual that the CSP examination is voluntary and may be terminated at any time. The examinee may not be compelled to submit to, or continue to take, a CSP examination.
- e. Advise the individual of the right against self-incrimination and the right to obtain and consult with legal counsel. Civilians may request a union representative's presence. If the counsel or union representative does not have the appropriate clearance or access, and the examination cannot be completed without discussion of classified material, the examination will be terminated.
- f. Obtain the individual's written consent to take a CSP examination. Without written consent, the CSP examination will not be conducted.
- g. Collect required health and biographic data.
- h. Explain the polygraph instrument, appropriate physiology and test procedures.
- i. Respond to the examinee's questions about the process.
- j. Formulate and review appropriate examination questions.

E-18. In-test phase

The in-test phase includes the collection and analysis of polygraph charts.

E-19. Post-test phase

- a. *NDI CSP examinations.* The examiner will advise the examinee of tentative NDI results. The examinee also will be informed that the CSP examination charts are subject to final quality control review and that it is sometimes necessary to conduct additional tests to confirm the NDI results.
- b. *DI and INC CSP examinations.* The examiner will conduct a post-test interview to assist the examinee in

resolving any problem with relevant CI topics. Whenever possible CSP examinations will be resolved by the post-test interview and additional testing by the same or different polygraph examiners. An initial DI or INC CSP examination may be resolved and a NDI conclusion reached. Include any reportable admissions in the PER and a sworn statement. If a CSP examination cannot be resolved by post-test interviews and additional testing, the unresolved CSP examination will be recorded as DI or INC. In such cases, the examinee will be advised that an investigation may be conducted.

c. Questionnaire. When the examination process is completed, the examinee will be asked to answer an anonymous questionnaire on the CSP program and return it to INSCOM.

Section III

Actions after the CSP examination

E-20. Processing CSP examination results

a. Quality control actions. A quality control review is conducted on all CSP examinations. NDI CSP examinations with no admissions will be filed in the IRR. All DI and INC PER will be forwarded to the ACCO. NDI PER containing admissions will also be forwarded to the ACCO.

b. Command notification. Following a CSP examination, commanders, program managers, and agency heads will be advised only that the individual has met his or her obligation to attend a scheduled CSP examination and not specific examination results. INSCOM will publish and disseminate a periodic listing of persons who have attended scheduled CSP examinations.

c. DI and INC CSP examinations of employment applicants. Non-government personnel applying for Government positions may be denied access to the information without investigation if the CSP examination results are DI or INC. Government employees applying for a position for which a CSP examination is required or requested may be investigated as described in paragraphs E-20 through E-22.

E-21. Referral for investigation

a. NDI and INC results. No investigation or further verification is authorized when the CSP examination result is NDI and there are no admissions recorded in the PER. Admissions made during the examination and recorded in the PER may be subject to further investigation, if they are clear and compelling investigative leads. The ACCO will review INC and NDI reports with admissions and determine whether or not to open a USAI investigation. The ACCO may request the appropriate investigative authority conduct a CI investigation on non-Army personnel. If the ACCO determines the admissions are not CI investigative leads, the ACCO will forward a copy of that PER to the individual's personnel security clearance determination authority. For INC results without admissions, the ACCO may review existing pertinent files and records to determine if investigative leads exist. If the ACCO determines that the existing information constitutes investigative leads, the ACCO will open an investigation.

b. DI CSP examination results.

(1) *FBI investigations.* The ACCO will refer DI cases on civilians, contractors, and consultants in the United States to the FBI headquarters. If the FBI accepts the referral, the FBI will open a preliminary inquiry and advise the ACCO of the results. If the FBI does not accept a DI referral for investigation, the ACCO will initiate or request a CI investigation to resolve the issues.

(2) *Army CI investigations.* The DOD component that conducted the CSP examination normally will conduct a CI investigation of military personnel and civilian personnel, contractor and consultant employees working outside the United States. USAI investigations will be closed within 120 days from opening. The ACCO may transfer investigative responsibility of non-Army military and personnel to the individual's parent military department if the department requests or accepts investigative jurisdiction. The ACCO will request investigation of DI referrals to other military departments be conducted within 120 days. The CI investigation may be extended beyond 120 days if credible derogatory information or additional investigative leads are developed.

c. Refusal investigations. Refusal cases will not routinely be investigated unless there is evidence that the refusal is an attempt to conceal matters of CI significance. The ACCO will determine when it is appropriate to conduct a CI investigation of refusals, based upon DOD 5210.48-R and the declination statement or memorandum. The ACCO may refer non-Army personnel refusals to the appropriate investigative authority.

E-22. After the investigation

a. ACCO actions. The ACCO will review the investigative results. Derogatory information of a criminal nature will be referred to the appropriate law enforcement agency. The ACCO will refer derogatory information of a suitability nature to the appropriate personnel security clearance determination authority. If a DI CSP examination report and investigation contain no actionable derogatory information, the results will be forwarded to HQDA (DAMI-CI).

b. Army requester actions. When HQDA advises an Army requester of a completed investigation on a DI exam, the requester will determine whether or not a SA personnel security determination is needed. If the requester decides that the investigation has confirmed the individual's trustworthiness, a SA determination is not required. The individual's access will continue and the Army requester has no further action. If the requester determines that even with due

consideration of the subsequent investigation, the Army individual's further access should be denied, a request must be forwarded via command channels through the DCSINT to the SA. The request will specify the extent of the Army individual's access and explain why the SA should deny the person further access based upon DI CSP examination charts that have not been confirmed by a follow-up investigation.

c. DCSINT actions. The DCSINT will process any denial requests on Army personnel.

d. SA unfavorable personnel security determinations. In these cases—

(1) A SA determination to deny access will be provided in writing. The Army individual also will be advised that the SA's determination may be appealed to the Secretary of Defense. Secretary of Defense determinations are final.

(2) An appeal to a SA decision must be filed within 60 days of notification. The appeal may contain any information that the appellant wishes the Secretary of Defense to consider in reaching a final determination.

(3) Copies of the SA's denial determination and notification to the Army individual may be retained only in the immediate office of the SA, ODCSINT, the IRR, and in the security office of the Army element responsible for controlling access to that information. This provision does not preclude use of these records in litigation. No other notifications are made.

E-23. CSP examination records administration

a. CSP technical documents. These documents include pre-test preparations, examiner notes, polygraph worksheet, polygraph examination charts, and other technical records. CSP technical documents may be filed with other materials in a related investigation. CSP technical documents will be removed before granting persons outside INSCOM polygraph channels access to the related investigative materials.

b. CSP examination reports. Record copies of PER may be filed in the IRR with related investigative records when a CI investigation is conducted. PER may be filed in any IRR dossier of the individual to whom the results pertain. The polygraph records will be maintained in such a manner as to segregate them from other dossier material. Nonrecord copies of the PER will be destroyed within 3 months from the date of completion of action for which release of nonrecord copies was authorized.

c. Refusal information. Information concerning a person's refusal to undergo a CSP examination will be protected UP AR 340-21. Refusal information will be forwarded to the ACCO and filed in the IRR for a minimum of 15 years. The fact that a person refused to take a CSP examination may be provided to the examination requester, and to the individual's commander, agency head, or security manager, for appropriate specific suspension of access. INSCOM will forward refusal summaries to HQDA (DAMI-CI) for submission to TMO.

d. Examination recordings. See paragraph E-11.

E-24. Release of CSP examination reports

a. Control of CSP examination results. CSP examination results are privileged information and release will be strictly controlled. CSP examination results apply to those data contained on, or attached to, the PER when placed in the subject file. These data include—

(1) A synopsis of the CSP examination.

(2) Brief identification and background information.

(3) Relevant CI questions asked and answered.

(4) The polygraph examiner's conclusion concerning determination of truth or deception and any admissions made during the CSP examination.

(5) Allied documents such as sworn statements or polygraph examination statements of consent.

b. Release of CSP examination technical documents. Technical documents collected or connected with CSP examinations will not be sent outside of INSCOM, except as required by law. Normally these technical documents are exempted from release under the provisions of Exemption 7 of the Freedom of Information Act per DOD 5400.7-R.

c. Release of CSP examination reports. The IRR may release CSP PER to the following:

(1) The SA; The Under Secretary of the Army; the Chief of Staff, Army; The Vice Chief of Staff, Army; the Director of the Army Staff; the DCSINT; and their immediate staff advisers.

(2) Commander, INSCOM, Deputy Commander, Chief of Staff, and their immediate staff advisers.

(3) Army, other service and DOD officials responsible for criminal investigations, CI investigations and operations, foreign intelligence operations, inspector general investigations or inquiries, personnel security investigations, and personnel security clearance determinations.

(4) DOD officials corresponding to those listed in (1) (2), and (3), above.

(5) Members of the National Foreign Intelligence Board, provided there is an official need for the material.

(6) Federal, state, and local law enforcement officials when an alleged violation of federal or state law is contained in the CSP examination report, and INSCOM approves the report for release.

(7) The examinee or his or her legal counsel, upon written request. Release of classified reports are subject to the provisions for safeguarding classified information per AR 380-5.

(8) The National Archives and Records Service, GSA, upon retirement of the IRR file.

d. Requests for release of CSP examination results. Requests for release of CSP examination reports will be sent through Headquarters, INSCOM, to the IRR. The IRR will release CSP examination reports only after INSCOM approval.

Glossary

Section I Abbreviations

ACCO

Army Central Control Office

ACE

Allied Command Europe

AGC

Army General Counsel

AMC

Army Materiel Command

AOC

Army Operations Center

AOR

area of responsibility

ARPERCEN

Army Reserve Personnel Center

ASPP

Acquisition Systems Protection Program

ATOIC

Antiterrorism Operations and Intelligence Cell

AWOL

absent without leave

B&C

badge and credentials

C-E

communications-electronics

C-SIGINT

Counter-Signals Intelligence

CG

Commanding General

CI

counterintelligence

CIA

Central Intelligence Agency

CINC

Commander in Chief

CINCUSAREUR

Commander in Chief, U.S. Army Europe

COMSEC

communications security

CONUS

continental United States

CSA

Chief of Staff, U.S. Army

CSP

counterintelligence scope polygraph

DA

Department of the Army

DACAP

Department of the Army Cryptographic Access Program

DCID

Director of Central Intelligence Directive

DCSINT

Deputy Chief of Staff for Intelligence

DCSPER

Deputy Chief of Staff for Personnel

DI

deception indicated

DIA

Defense Intelligence Agency

DIRNSA

Director, National Security Agency

DIS

Defense Investigative Service

DOD

Department of Defense

DOJ

Department of Justice

EEFI

Essential Elements of Friendly Information

FBI

Federal Bureau of Investigation

FCI

Foreign Counterintelligence

FIS

foreign intelligence and security services

IMINT

Imagery Intelligence

HQDA

Headquarters, Department of the Army

HUMINT

Human Intelligence

IIR

Intelligence Information Report

INC

inconclusive

INSCOM

Intelligence and Security Command

IRR

Investigative Records Repository

LEA

law enforcement agency(ies)

LLSO

Low level source operations

MACOM

major Army command

MCM

Manual for Courts-martial

MI

Military Intelligence

MOS

military occupational specialty

MOU

memorandum of understanding

NCIC

National Crime Information Center

NDI

no deception indicated

NO

no opinion

NSA

National Security Agency

ORCON

Originator Controlled

PER

Polygraph Examination Report

PERSCOM

Personnel Command

PIR

Priority Intelligence Requirements

PM

provost marshal

PSI

personnel security investigation

RC

Reserve Components

RDTE

Research, Development, Test and Evaluation

SA

Secretary of the Army

SAEDA

Subversion and Espionage Directed Against the Army

SAP

special access program

SCA

special category absentee

SCO

sub-control office

SIGINT

Signals Intelligence

SJA

Staff Judge Advocate

SMU

special mission unit

SOFA

Status of Forces Agreement

SOI

Summary of Information

SSI

specialty skill identifier

SSN

Social Security Number

TAREX

target exploitation

TJAG

The Judge Advocate General

TMO

Technology Management Office

TRADOC

Training and Doctrine Command

TS
TOP SECRET

TSCM
technical surveillance countermeasures

TUSA
Third United States Army

UCMJ
Uniform Code of Military Justice

USACIDC
United States Army Criminal Investigation Command

USAI
United States Army Intelligence

USAIC
United States Army Intelligence Center

USAITAC
United States Army Intelligence and Threat Analysis Center

USAMPOA
U.S. Army Military Police Operations Agency

USARPAC
U.S. Army Pacific Command

USARSO
U.S. Army South

USASOC
U.S. Army Special Operations Command

USC
United States Code

Section II

Terms

The following definitions are applicable to this regulation only, unless marked with the original source.

admission

A polygraph examinee's acknowledgement of a fact, or a culpable statement associated with a relevant issue.

affiliation with the Department of Defense

Persons, groups of persons, or organizations are considered to be affiliated with the Department of Defense if they are:

- a.* employed by, or contracting with, the DOD or any activity under the jurisdiction of DOD, whether on a full-time, part-time, or consultative basis;
- b.* members of the Armed Forces on active duty, National Guard members, or those in a reserve or retired status;
- c.* residing on, authorized access to, or conducting or operating any business or other function at any DOD installation or facility;
- d.* authorized access to defense information;
- e.* participating in other authorized DOD programs; or
- f.* applying or being considered for any status described above. (Joint Pub 1-02)

analysis

A step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation. (Joint Pub 1-02)

apprehension

1. The taking of a person into custody, the military equivalent of “arrest.”
2. The restraint of a person by oral or written order not imposed as punishment, directing the person to remain within specified limits. (Rule 304, MCM)

assassination

The murder or attempted murder of DOD personnel, for political or retaliatory reasons, by terrorists or agents of a foreign power.

Badge and Credential Controller

The individual responsible for day-to-day management of the Military Intelligence Badge and Credential Program. This person maintains the central records of personnel eligible for B&C; sees to the production of badges and credential blank forms; central storage, issuance and inventory of B&C and representative credentials; and manages the Badge Trophy Program.

Badge and Credential Custodian

Advisor to the unit commander and the individual responsible for day-to-day management of a unit B&C account. Ensures the eligibility of and requirement for issue to unit personnel, receives from and ships to the B&C central repository, conducts physical inventories, provides temporary storage, and establishes and inspects sub-accounts.

biographical intelligence

That component of intelligence which deals with individual foreign personalities of actual or potential importance. (Joint Pub 1-02)

case

1. Record of the development of an intelligence operation, including personnel, modus operandi, and objectives. (Joint Pub 1-02)
2. Records of a counterintelligence investigation, special operation, or low level source operation.

chart

A complete recording of physiological responses to a series of questions asked while the polygraph instrument is operating. Measures respiratory, cardiovascular, and electrodermal activity. (DOD Polygraph Test Program SOP)

closed investigation

A case in which there is no further investigative activity, reports have been finalized and final disposition of the case file has been completed.

collection requirement

1. An established intelligence need considered in the allocation of intelligence resources to fulfill the essential elements of information and other intelligence needs of a commander. (JCS Pub 1-02)
2. An expression of an intelligence information need that requires collection and carries at least an implicit authorization to commit resources in acquiring the needed information. (Intelligence Community Staff Glossary of Intelligence Terms and Definitions)

combatting terrorism

Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. (Joint Pub 1-02)

counterespionage

That 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 activities. (Joint Pub 1-02)

counterespionage project

Efforts focused on known FIS methodology and/or suspected or known FIS personalities to detect espionage directed against the U.S. Army.

counterintelligence

1. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist

activities, but not including personnel, physical, document or communications security programs. Synonymous with foreign counterintelligence. (ICS Glossary)

2. Those activities which are concerned with identifying and counteracting the threat to security posed by foreign intelligence services or organizations, or by individuals engaged in espionage, sabotage, sedition, subversion or terrorism.

counterintelligence aspects

Those elements of a non-intelligence investigation that are of counterintelligence interest, such as evidence of coercion, gathering of classified or sensitive information, solicitation of information, deliberate unauthorized disclosure of classified information, or indications of affiliation with FIS. CI aspects are often hard to readily distinguish, but tend toward intelligence collection/operations as opposed to criminal actions.

counterintelligence collection

1. The systematic acquisition of information on espionage, sabotage, terrorism, and related foreign intelligence activities conducted for, or on behalf of, foreign powers, organizations, or persons, that are directed against or threaten DOD interests. (DOD 5240.10)

2. The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. (Joint Pub 1-02)

3. The acquisition of information by means of direct observation, liaison, solicitation, or exploitation of sources in response to approved collection requirements, when such has been made a part of the files or holdings of an intelligence component.

counterintelligence controlled activities

CI activities managed or monitored through a centralized control system, including offensive CI operations, CI investigations, CE projects, low level source operations, defensive source programs, TSCM, intelligence polygraph, and use of special techniques.

counterintelligence investigation

A duly authorized, systematic, detailed examination or inquiry to uncover facts and determine the truth of a matter regarding a person or other entity which is or may have engaged in espionage or other clandestine intelligence activity, sabotage, sedition, subversion, terrorist activities, or assassinations conducted by, or on behalf of, a foreign power, or unauthorized disclosures of classified information. This may include collecting, processing, reporting, storing, recording, analyzing, evaluating, producing and disseminating the authorized information.

counterintelligence operations

Activities taken to hinder the multidisciplinary activities of foreign intelligence and security services, and to cause FIS to doubt the validity of its own analysis.

counterintelligence special agent

Soldiers holding the SSI 35E, MOS 351B or 97B, and civilian employees in the GS-0132 career field, who have successfully completed a CI officer/agent course, who are authorized USAI badges and credentials, and who are assigned to conduct CI investigations and operations. Also known as CI agent or MI agent.

counterintelligence special operations

Those operations involving direct engagement with known or suspected FIS through human source or technical efforts. These include offensive counterintelligence operations, counterespionage projects, defensive source programs, and investigative special techniques.

countermeasures

1. That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (Joint Pub 1-02)

2. Defensive security programs and activities which seek to protect against both foreign intelligence collection efforts and unauthorized access to, or disclosure of, protected facilities, information, and material. (ICS Glossary)

countersabotage

That aspect of counterintelligence designed to detect, destroy, neutralize, or prevent sabotage activities through identification, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting sabotage activities. (Joint Pub 1-02)

counter-signals intelligence

Actions taken within the Army CI Program to determine the foreign signals intelligence threat, collect and identify

friendly C–E vulnerabilities, develop recommendations to counteract hostile exploitation, and evaluate the effectiveness of applied countermeasures.

countersubversion

That aspect of counterintelligence designed to detect, destroy, neutralize, or prevent subversive activities through the identification, exploitation, penetration, manipulation, deception, and repression of individuals, groups, or organizations conducting or suspected of conducting subversive activities. (Joint Pub 1–02)

cover

Those measures necessary to give protection to a person, plan, operation, formation or installation from the enemy intelligence effort and leakage of information. (Joint Pub 1–02)

debriefing

Interviewing, under other than hostile conditions, of an individual who has completed an intelligence assignment or who has knowledge—through observation, participation, or otherwise—of operational intelligence or counterintelligence significance. (ICS Glossary)

deception

Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Joint Pub 1–02)

defector

1. National of a country who has escaped from the control of such country or who, being outside such jurisdiction and control, is unwilling to return thereto and is of special value to another country. (Article 85, UCMJ and Joint Pub 1–02)

2. (NATO) A person who repudiates his or her country when beyond its jurisdiction or control. (Joint Pub 1–02)

3. Conscious (mental and/or physical) abandonment of loyalty, allegiance, duty, or principal to one's country. (ICS Glossary)

deliberate compromise

The act, attempt, or reported contemplation of intentionally conveying classified documents, information, or material to any unauthorized person, including unauthorized public disclosure. (18 USC 798)

Department of the Army civilian personnel

All U.S. citizen officials and employees of the Army not on active military duty, and all foreign nationals employed by the Army.

Department of the Army Cryptographic Access Program

A formal program for personnel who require access to certain U.S. classified cryptographic information. Included in this program are personnel with access to any keying material classified TOP SECRET; descriptions, specifications, and/or drawings of cryptographic logic; key generating software; key supporting Special Operations Forces, special access programs, joint or combined operations; full maintenance manuals classified SECRET or higher; and personnel who prepare, authenticate, or decode valid or exercise nuclear control orders. (AR 380–40)

detainee

Any person captured or otherwise detained by an armed force. (Joint Pub 1–02)

doctrine

Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application. (Joint Pub 1–02)

espionage

1. The act of obtaining, delivering, transmitting, communicating, or receiving information in respect to the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. (18 USC 792–798 and Article 106a, UCMJ)

2. Actions directed toward the acquisition of information through clandestine operations.

3. Overt, covert, or clandestine activity designed to obtain information relating to the national defense with intent or reason to believe that it will be used to the injury of the United States or to the advantage of a foreign nation. (Joint Pub 1–02)

favorably resolved

A polygraph examination result when there is no deception indicated, and in which no derogatory information requiring action is obtained.

force protection

Security program designed to protect soldiers, civilian employees, family members, facilities and equipment, in all locations and situations; accomplished through planned and integrated application of operations security, combatting terrorism, physical security, base defense, personal protective services, law enforcement and crime prevention, and supported by intelligence, counterintelligence, and other security programs. (AR 525–13)

incapacitation

The deliberate or attempted infliction of severe mental or bodily harm of DOD personnel, for political or retaliatory reasons, by terrorists or agents of a foreign power.

investigative stop

The lawful, temporary detention of a person when the detainer has information or observes unusual conduct that leads him to reasonably conclude, in light of his experience, that criminal activity is afoot. The purpose of the stop must be investigatory in nature. (Military Rules of Evidence 314(f)) CI agents may make investigative stops regarding activity for which USAI has investigative authority.

local operational data

Information which is used to sustain other internal CI activities. Examples include general information on local liaison contacts, location maps, significant activities and facilities, intelligence nuisances, and supported units.

low level source operations

Non-clandestine operations to collect, on behalf of the Army theater component commander, low level information on local activities which may influence the protection of deployed U.S. forces.

modus operandi

A method of operating.

National Foreign Intelligence Board

A body formed to advise the Director of Central Intelligence on

1. production, review and coordination of national foreign intelligence;
2. interagency exchanges of intelligence information;
3. arrangement with foreign governments on intelligence matters;
4. protection of intelligence sources and methods;
5. activities of common concern; and
6. other matters referred to it by the DCI. (EO 12356)

open investigation

One in which exploitable leads are being pursued. Open cases also include those that are in suspended or terminated status.

production

1. Conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. (Joint Pub 1–02)
2. The process of collating, evaluating, interpreting and analyzing information of counterintelligence significance and publishing studies, assessments, estimates, and reports. (DOD 5240.10)

protective services

Those security measures taken to protect an individual designated by a MACOM commander as high risk level I (HRP I), which may include personal security, site and conference security, application of appropriate physical security measures, and use of specialized protection techniques, such as motorcades and countersurveillance. Such services are provided in the Army by USACIDC or MP personnel.

sabotage

1. An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources. (18 USC 2151–2156, Article 108, UCMJ, and Joint Pub 1–02)

2. Action against material, premises, or utilities, or their production, which injures, interferes with, or obstructs the national security or ability of a nation to prepare for or carry on a war. (ICS Glossary)

sedition

Participation, in concert with another person or persons, in one or more of the following:

- a. Knowingly or willfully advocating or teaching the duty or necessity of overthrowing the U.S. government or any political subdivision therein by force or violence.
- b. Printing, publishing, circulating, selling or publicly displaying written matter, with intent to cause the overthrow or destruction of any such government, which advocates or teaches the duty or necessity of such overthrow by force or violence.
- c. Organizing a society or group whose purpose is to advocate or teach the duty or necessity of such overthrow by force or violence.
- d. Being or becoming a member of, or affiliated with, such society or group, knowing the purpose thereof. (18 USC 2384–2385 and Article 94, UCMJ)

special access program

A sensitive activity, approved by the Secretary of the Army, imposing a “need-to-know” or access controls beyond those normally required for access to CONFIDENTIAL, SECRET, or TOP SECRET information. (AR 380–381)

special category absentee

Any soldier reported AWOL who has had access to TOP SECRET information during the last 12 months or is currently assigned to a special mission unit. An absentee within this criteria is immediately reported as a deserter regardless of the length of absence. (AR 190–9, AR 630–10)

special mission unit

A unit assigned a mission of such extraordinary sensitivity as to require specific centralized management, oversight, and employment considerations. (AR 525–17)

spying

In time of war, the act of clandestinely or under false pretenses collecting or attempting to collect information with the intent to convey it to a hostile party. (Article 106, UCMJ)

subject

A person or other entity about whom a CI investigation is conducted.

subversion

- 1. Actively encouraging military or DOD civilian personnel to violate laws, disobey lawful orders or regulations, or disrupt military activities, with the willful intent thereby to interfere with, or impair the loyalty, morale, or discipline of US military forces.
- 2. Lending aid, comfort, and moral support to individuals, groups or organizations that advocate the overthrow of the US government.
- 3. All willful acts intended to be detrimental to the best interests of the US government which do not fall into the categories of treason, sedition, sabotage, or espionage. (18 USC 2387–2388 and Article 134, UCMJ)
- 4. (DOD) Action designed to undermine the military, economic, psychological, political strength or morale of a regime.
- 5. (NATO) Action designed to weaken the military, economic or political strength of a nation by undermining the morale, loyalty or reliability of its citizens. (Joint Pub 1–02)

suspended investigation

An open investigation in which all available information has been received, yet there remains a likelihood that new information may be available in the future.

technical control

An objective system of oversight, ensuring complete and proper accounting of CI investigative and operational activities, compliance with established policy, and quality assurance.

technical surveillance countermeasures

Techniques and measures to detect and neutralize a wide variety of FIS penetration technologies that are used to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and transmission medium, or the use of

various types of stimulation or modification to equipment or building components for direct or indirect transmission of information meant to be protected. (ICS Glossary)

terminated investigation

An open investigation in which all known exploitable leads have been exhausted and reports have been forwarded to the ACCO.

terrorism

1. The unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives. (Joint Pub 1–02)

2. The use or threat of force or violence by sub-national groups or clandestine state agents in a manner calculated to induce a psychological state, usually fear, in an audience wider than the direct victim, for the claimed purpose of causing some kind of social or political response.

threat assessment

An evaluation of the current or projected capability of a foreign intelligence service to limit, neutralize, or negate the effectiveness of a friendly mission, organization, or material item through multidisciplined intelligence collection efforts, espionage, or sabotage.

treason

1. Violation of the allegiance owed to one's sovereign or state; betrayal of one's country. (18 USC 2381, Article 104, UCMJ, and Joint Pub 1–02)

2. Aiding or attempting to aid the enemy with arms, ammunition, supplies, money, or other things.

3. Without proper authority, knowingly harboring or protecting or giving intelligence to, communicating or corresponding with or holding any intercourse with the enemy, either directly or indirectly. (18 USC 2381 and Article 104, UCMJ)

unauthorized disclosure

A communication or physical transfer of classified information to an unauthorized recipient. An unauthorized recipient is someone with no security clearance; one with a security clearance but no need to know the information; a foreign intelligence and security service; the press; criminal elements—any person or organization who is not routinely authorized access to U.S. classified information and who does not absolutely require that information to accomplish a mission in support of U.S. national security.

vulnerability assessment

The process of identifying weaknesses in the protection of friendly operations and activities which, if successfully exploited by foreign intelligence efforts, could compromise current or future plans, capabilities, or activities. This includes research, development, testing and evaluation.

Section III

Special Abbreviations and Terms

This section contains no entries.

Index

This index is organized alphabetically by topic and by subtopic within a topic. All are identified by paragraph number.

Abbreviations, 1–3, Glossary

Access to military privileges, 8–7

Access to records, information and facilities, 8–15

Advice and assistance, 5–6

Affiliation with the Department of Defense, definition, Glossary

Analysis, 7–1, 7–2, Glossary

Antiterrorism Operations and Intelligence Cell

address, C–5

reports to, 2–8, 2–9, 2–10, 2–11, 2–13

Apprehension

Authority, 8–12

Definition, Glossary

Army Central Control Office

address, C–4

responsibilities, 3–2, E–21, E–22

Army General Counsel, 2–1

Army requesters of CI scope polygraphs, E–5, E–6, E–22

Assassination, 4–2, Glossary

Assignment of CI personnel, 8–2

Authority

Apprehension, 8–12

Army CI, 1–4

Oath administration, 8–11

Search and seizure, 8–13

Badges and Credentials

Accountability, 9–2

Badge trophy program, 9–2, 9–9

Central repository, 9–8

Controller, 9–6, 9–8, Glossary

Criteria for issue of representative credentials, 9–4

Custodian/sub-custodian, 9–2, 9–3, 9–7, 9–8, Glossary

Fabrication, unauthorized, 4–7

General, 9–1

Initial B&C issue by other than USAIC, 9–5

Inventories, 9–2

Issue and retention of badges and credentials, 9–3

Loss, 9–6

Misuse, 4–7, 9–7

Responsibilities, 9–2, 9–5, 9–8

Biographical intelligence, 7–2, Glossary

Case, definition, Glossary

CI scope polygraphs

Authorized uses, E–4

Centralized program management, E–3

Conclusions, E–8

Controls, E–6

Examiners, 10–3, E–14

General, E–1

Investigations, E–21

Medical suitability for, E–12

Monitoring, E–11

Notification, E–15

Other agency examinations, E–13

- Pre-test interview, E-17
- Processing results, E-20
- Prohibitions, E-6
- Purpose, E-2
- Questions, E-7
- Recording, E-11
- Records administration, E-23
- Referral for investigation, E-21
- Refusals, E-6, E-10, E-21, E-23
- Release of reports, E-24
- Reporting admissions, E-9
- Responsibilities, E-5
- Selection, training and certification of polygraphers, 10-3
- Terminations, E-6, E-10
- Topics, E-7
- Use, 10-2
- Civil disturbances, 5-12**
- Civil legal proceedings, 8-14**
- Classification guides, B-2**
- Clothing and rank, 8-5**
- Collection**
 - Civil disturbances, 5-12
 - Debriefings and interrogations, 6-5, 6-6
 - Definition, Glossary
 - General, 6-1
 - Local operational data, 6-4, Glossary
 - Procedures, 6-3
 - Reporting, 6-3
 - Requirement, 6-1, 6-2, Glossary
 - Returned U.S. defector debriefings, 6-6
 - Validating requirements, 6-2
- Combatting terrorism, 5-4, Glossary**
- Commanders, 2-14, 2-17, 9-2, 9-4, 9-5, 9-7, D-2, E-5, E-6, E-22**
- COMSEC monitoring, 5-15**
- Control offices**
 - Army Central Control Office, 3-2, E-21, E-22
 - General, 3-1
 - Sub-control offices, 3-3
- Counterespionage, definition, Glossary**
- Counterespionage project, 5-1, Glossary**
- Counterintelligence**
 - Aspects, 4-2, Glossary
 - Collection, 6-1, 6-2, 6-3, Glossary
 - Controlled activities, 3-1, Glossary
 - Investigation, 4-1, 4-2, 4-5, 4-6, 4-7, 4-9, Glossary
 - Mission, 1-5
 - Operations, 5-1, 5-2, 5-3, Glossary
 - Policy, 1-5
 - Special Agent, definition, Glossary
 - Special operations, 5-1, Glossary
- Countermeasures, 5-15, 5-17, Glossary**
- Countersabotage, definition, Glossary**
- Counter-SIGINT**
 - Definition, Glossary
 - General, 5-14
 - C-SIGINT support, 5-15

- in Red Team operations, 5–18
- Countersubversion, definition, Glossary**
- Courtesy Letter Program**
 - Disposition, D–5
 - Format, D–6
 - General, D–1
 - Local inquiries, D–4
 - Procedures, D–3
 - Responsibilities, D–2
- Cover, 5–17, 8–5, Glossary**
- Covering agent support, 5–19**
- Criminal Investigation Command**
 - responsibilities, 2–13, 4–7
 - shared investigative jurisdiction, 4–5
- Debriefing, 4–2, 4–5, 6–5, 6–6, B–5, Glossary**
- Deception, 5–3, Glossary**
- Defector, 6–5, 6–6, Glossary**
- Defense Investigative Service, 2–8, 2–9, 2–11, 2–12, 4–3, D–2**
- Deliberate compromise, definition, Glossary**
- Department of the Army civilian personnel, definition, Glossary**
- Department of the Army Cryptographic Access Program, 4–2, Glossary**
- Deputy Chief of Staff for Intelligence**
 - responsibilities, 2–4, 9–2, E–5
 - address, C–1
- Deputy Chief of Staff for Personnel, 2–5, E–5**
- Detainee, 4–2, 6–5, Glossary**
- Doctrine, 2–6, Glossary**
- DOD-affiliated, definition, Glossary**
- Eighth U.S. Army, 2–8**
- Espionage, definition, Glossary**
- Evaluation reports, B–4**
- Federal Bureau of Investigation**
 - At U.S. missions abroad, 4–6
 - General jurisdiction, 4–2, 4–7, E–21
 - National Crime Information Center, 4–8
 - Reports to, 4–4, 4–6
- Field operating agencies/activities, 2–14, E–5**
- Forces Command, 2–8**
- Force protection, 5–3, Glossary**
- Hostile intelligence simulation (Red Team), 5–17**
- Incapacitation, 4–2, Glossary**
- Inspector General, the, 2–2**
- Intelligence Center, 9–2**
- Intelligence and Security Command**
 - responsibilities, 2–11, 9–2, E–5
 - address, C–2
- Intelligence Information Reports, 6–3**
- Intelligence polygraphs**
 - CI scope, 10–2, appendix E
 - Requesting support, 10–4
 - Selection, training and certification of polygraphers, 10–3
 - Use of, 10–2
- Interrogations, 6–5**
- Investigative stop, 8–12, Glossary**

Investigations

- Army CI investigative jurisdiction, 4-2, 4-6, E-21
- Closed, definition, Glossary
- Definition, Glossary
- General, 4-1
- Geographic jurisdiction, 4-5
- Joint investigations, 4-5
- Open, definition, Glossary
- Personnel authorized to conduct, 4-1
- Personnel security, 4-3
- Release of investigative information, 4-9, E-24
- Reporting requirements, 4-4
- Shared investigative responsibility, 4-5
- Suspended, definition, Glossary
- Terminated, definition, Glossary

Joint investigations, 4-5

Judge Advocate General, the, 2-3

Local operational data, 6-4, Glossary

Low level source operations, 5-4, Glossary

Major Army Commands, 2-14, E-5

Major subordinate commands, 2-14

Materiel Command, 2-7

Military Police Operations Agency, 2-13

Mission, 1-5

National Crime Information Center, 4-8

National Foreign Intelligence Board, E-24, Glossary

National Guard Bureau, responsibilities, 2-15

Natural disaster operations, 5-13

Operations

- Advice and assistance, 5-6
- CI special operations, 5-1, Glossary
- CI support to acquisition and special access programs, 5-8
- CI support to domestic civil disturbances, 5-12
- CI support to force protection, 5-4
- CI support to HUMINT, 5-9
- CI support to natural disaster operations, 5-13
- CI support to treaty verification, 5-10
- CI technical support activities, 5-7
- Liaison, 5-11
- Low level source, 5-5

Oversight, intelligence, 1-5, 2-1, 2-2, 2-4, E-5

Personnel

- Access to military privileges, 8-7
- Assignment, 8-2
- Billets, 8-8
- Clothing and grade, 8-5
- Debriefing, B-5
- Duty limitations, 8-3
- Evaluation reports, B-4
- Impersonation of, 4-7
- Mess, 8-8
- Nonstandard spectacles, 8-6
- Records screening, B-6
- Selection as polygraphers, 10-3

- Temporary duty, 8–8
- Weapons, 8–9
- Withdrawal of CI specialty, 8–4
- Personnel Command, 2–5, 9–2**
- Policy, 1–5**
- Polygraphs**
 - Admission, definition, Glossary
 - Chart, definition, Glossary
 - Favorably resolved, definition, Glossary
 - General, 10–1
 - Requesting, 10–4
 - Selection, training and certification of polygraphers, 10–3
- Production, 7–3, Glossary**
- Protective services, definition, Glossary**
- Provost Marshal, shared investigative jurisdiction, 4–5**
- Publicity, B–3**
- Red Team operations, 5–17**
- References, appendix A**
- Reports**
 - Collection, 6–3
 - Criminal information, 4–4
 - Evaluations, B–4
 - Investigations, 4–4, E–22, E–23
 - Release of, 4–9, E–24
 - Unit roster for B&C, 9–8
- Reserve Components schools, 9–5**
- Reserve Components unit commanders, 9–8**
- Reserve Personnel Center, responsibilities, 2–5, 9–2**
- Sabotage, definition, Glossary**
- Secretary of the Army, E–5**
- Security**
 - Classification guides, B–2
 - Debriefing, B–5
 - Evaluation reports, B–4
 - Publicity, B–3
 - Screening personnel records, B–6
- Sedition, definition, Glossary**
- Special access programs, 5–8, 10–2, E–4, Glossary**
- Special Agents**
 - Access to records, information and facilities, 8–15
 - Apprehension authority, 8–12
 - Assigned to Special Mission Units, 8–16
 - Civil legal proceedings, 8–14
 - Definition, Glossary
 - Freedom of movement, 8–10
 - Oath administration, 8–11
 - Search and seizure authority, 8–13
 - Selection, training and certification as polygraphers, 10–3
- Special category absentee, 4–2, 4–5, Glossary**
- Special Operations Command, 2–10**
- Special mission unit, 8–16, Glossary**
- Spying, definition, Glossary**
- Sub-control offices, 3–3**
- Subject, definition, Glossary**
- Subversion, definition, Glossary**

Technical control, 3–1, Glossary
Technical support activities, 5–6
Technical surveillance countermeasures, 5–7, Glossary
Techniques
 Covering agent, 5–19
 General, 5–16
 Hostile intelligence simulation (Red Team), 5–18
 Vulnerability assessments, 5–17, 7–3, Glossary
Terms, 1–3, Glossary
Terrorism, definition, Glossary
Third U.S. Army, 2–9
Threat assessment, 7–2, 7–3, Glossary
Training and Doctrine Command, 2–6
Treason, definition, Glossary
Unauthorized disclosure, 4–2, Glossary
U.S. Army Europe, 2–8
U.S. Army Forces Command, 2–8
U.S. Army Intelligence and Security Command, 2–11, 9–2, C–2, E–5
U.S. Army Intelligence and Threat Analysis Center, 2–16, C–3
U.S. Army Intelligence Center, 9–2
U.S. Army Materiel Command, 2–7
U.S. Army Pacific, 2–8
U.S. Army Reserve, 2–15
U.S. Army Reserve Command, 2–15
U.S. Army South, 2–8
U.S. Army Special Operations Command, 2–10
Vulnerability assessment, 5–17, 7–3, Glossary
Weapons, 8–9
650th MI Group, 2–12, 5–2, 5–7

UNCLASSIFIED

PIN 004116-000

USAPA

ELECTRONIC PUBLISHING SYSTEM

OneCol FORMATTER .WIN32 Version 175

PIN: 004116-000

DATE: 05-15-02

TIME: 11:41:28

PAGES SET: 63

DATA FILE: C:\Wincomp\r381-20.fil

DOCUMENT: AR 381-20

DOC STATUS: NEW PUBLICATION