Army Regulation 381–10

Military Intelligence

U.S. Army Intelligence Activities

Headquarters
Department of the Army
Washington, DC
3 May 2007

UNCLASSIFIED

SUMMARY of CHANGE

AR 381–10
U.S. Army Intelligence Activities

This rapid action revision, dated 3 May 2007--

- Cancels the protective marking FOR OFFICIAL USE ONLY.
- Changes major Army command to Army Command, Army Service Component Command, and Direct Reporting Unit throughout the publication.
- Delineates Army Intelligence Components (para 1-1).
- Changes major Army command to Commanders, U.S. Army Intelligence and Security Command and 650th MI Group (para 1-9b).
- Rescinds Computer Trespassers (para 5-16).
- Addresses the consensual intercept of computer trespasser communications and the approval requirements (paras 5-17 and 5-18).
- Adds a provision addressing nonconsensual physical searches of non-U.S. persons outside the United States and the approval authorities (paras 7-4 and 7-5b).
- Clarifies responsibility of commanders to provide access to personnel conducting oversight functions (para 14-3c).
- Clarifies reporting requirements for questionable intelligence activity under Procedure 15 (paras 15-2b, 15-2c(1), 15-2c(4), 15-2d, 15-2e, 15-3a(1), and 15-6c).
- Clarifies requirements for recurring intelligence oversight reporting (paras 15-6d, 15-6d(1), and 15-6d(2)).

This major revision, dated 22 November 2005--

- Adds Army Reserve and Army National Guard responsibilities (paras 1-4k through n).
- Delineates Army intelligence components (para 1-2).
- Adds internet considerations and computer trespassers (paras 1-8, 5-4a, 5-4c, and 5-21).

- Requires the intelligence oversight staff officer to be an intelligence professional (paras 1-4h(7), 1-4i(6), 1-4j(7), 1-4k(6), 1-4m(6), 1-4n(2), and 1-4p(4).

- Expands approval authorities (paras 4-3, 5-7b, 5-8c, 5-20b, 6-4, 7-1a(1), 7-2a(1), 8-3c, 8-3d, 8-4c, 9-4b, 9-5a, 9-5b, and 10-4a).

- Clarifies reporting for questionable intelligence activities (paras15-1, 15-2a, 15-2c through 15-2l, 15-4a and b, and 15-5).

- Clarifies reporting for Federal crimes (paras 16-1, 16-2, and 16-3).

- Adds guidance on force protection support limitations within the United States (paras 17-1 and 17-2).

- Adds guidance on U.S. Army Intelligence participation in multinational intelligence activities (para 17-3).

- Adds guidance on U.S. Army Intelligence participation in joint intelligence activities (para 17-4).

- Adds guidance on U.S. Army Intelligence support to other Department of Defense investigative organizations (para 17-5).

- Changes references to DOD intelligence components and Department of Defense agencies to Army intelligence components and Army agencies throughout, to reflect accurately the applicability of this regulation.

Headquarters
Department of the Army
Washington, DC
3 May 2007

*Army Regulation 381–10

Effective 3 June 2007

Military Intelligence

U.S. Army Intelligence Activities

By Order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the Secretary of the Army

History. This publication is a rapid action revision. The portions affected by this rapid action revision are listed in the summary of change.

Summary. This regulation implements Executive Order 12333, as amended by Executive Orders 13284 and 13355; policy between the Department of Justice and intelligence community members on crimes reporting; and Department of Defense Directive 5240.1, Department of Defense Publication 5240.1–R, and Department of Defense Instruction 5240.4. It establishes responsibility for intelligence activities concerning U.S. persons, includes guidance on the conduct of intrusive intelligence collection techniques, and provides reporting procedures for certain Federal crimes.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the United States Army Reserve, unless otherwise stated. During mobilization, the Deputy Chief of Staff, G–2 may modify chapters and policies contained in this regulation.

Proponent and exception authority. The proponent for this regulation is the Deputy Chief of Staff, G–2. The Deputy Chief of Staff, G–2 has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The Deputy Chief of Staff, G–2 may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the benefits and must include a formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army management control process. This regulation contains key management control provisions and identifies key management controls that must be evaluated.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–2 (DAMI–CDC), 1000 Army Pentagon, Suite 2D350, Washington, DC 20310–1000.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff, G–2 (DAMI–CDC), 1000 Army Pentagon, Suite 2D350, Washington, DC 20310–1000.

Committee Continuance Approval. The establishment and/or continuance of Army committees are made in accordance with Army Regulation 15–1. The regulation requires that the proponent justify establishing and/or continuing the committee(s), coordinate draft publications, and coordinate changes in committee status with the DA Committee Management Office, ATTN: SAAA-RP, Office of the Administrative Assistant, Resources and Programs Agency, 2511 Jefferson Davis Highway, Taylor Building, 13th Floor, Arlington, VA 22202-3926; and, if it is determined that an established "group" identified within this regulation later takes on the characteristics of a committee, the proponent will follow all Army Regulation 15–1 requirements for establishing and continuing the group as a committee. The Department of the Army Committee Management Officer has reviewed this regulation and concurs in the establishment and/or continuance of committee(s) outlined herein.

Distribution. This publication is available in electronic media only and is intended for command levels A, B, C, D, and E for the Active Army, the Army National Guard/Army National Guard of the United States, and the United States. Army Reserve.

*This regulation supersedes AR 381–10, dated 22 November 2005.

Contents (Listed by paragraph and page number)

Contents—Continued

Contents—Continued

Contents—Continued

Appendixes

Glossary

Chapter 1
General

1–1. Purpose

This regulation enables any Army component performing authorized intelligence functions to carry out those functions in a manner that protects the constitutional rights of U.S. persons. It also provides guidance on particular collection techniques to obtain information for foreign intelligence or counterintelligence purposes. Army intelligence components include the following Active Army, Army Reserve, and Army National Guard (ARNG) activities:

a. Office of the Deputy Chief of Staff, G–2.

b. U.S. Army Intelligence and Security Command and subordinate units.

c. 650th Military Intelligence (MI) Group, Supreme Headquarters Allied Powers Europe.

d. Senior intelligence officers and staff of Army Commands (ACOM), Army Service Component Commands, and Direct Reporting Units (DRU), and other commands and organizations.

e. G–2/S–2 offices.

f. Installation, organization, or facility security offices when carrying out intelligence activities.

g. MI units.

h. U.S. Army Intelligence Center and other organizations conducting intelligence training.

i. Intelligence systems developers when testing systems.

j. Contractors of any Army entity when conducting intelligence activities as defined in this regulation.

k. Any other Army entity when conducting intelligence activities as defined in this regulation.

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. Responsibilities

a. The Army General Counsel (AGC). The AGC is the legal counsel to the Secretary of the Army and the chief Department of the Army (DA) legal officer. AGC responsibility extends to any subject of law and other matters as directed by the Secretary. The AGC will—

(1) Exercise the Secretary of the Army's oversight of intelligence activities and monitor sensitive Army intelligence activities for legality and propriety.

(2) Review intelligence issues before any Secretariat official decision.

(3) Conduct all formal Army coordination with Department of Justice senior officials.

(4) Approve certain activities as listed in this regulation.

(5) Forward reports of Federal crimes that meet the Attorney General's guidelines for reporting through the Department of Defense (DOD) General Counsel to the Department of Justice.

(6) Review all matters that raise questions of interpretation concerning the procedures and activities covered by this regulation.

(7) Review, in coordination with The Judge Advocate General, all requests for exception, waiver, modification, or amendment of policies and procedures covered by this regulation.

b. The Inspector General (TIG). TIG will—

(1) Exercise oversight of intelligence activities as prescribed by AR 20–1 and this regulation.

(2) Maintain liaison with the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD–IO).

(3) Receive and process all reports required under chapter 15 and investigate or forward to appropriate authorities for investigation.

(4) Ensure reports of questionable intelligence activities are forwarded to appropriate officials as required.

(5) Prepare a quarterly report to ATSD–IO, describing significant questionable intelligence activities reported during that quarter, and any resultant actions. Include significant intelligence oversight activities and inspections, and suggestions for improvements in the oversight system.

c. The Judge Advocate General (TJAG). TJAG will—

(1) Provide legal advice directly to the Chief of Staff of the Army and members of the Army Staff and legal advice to the Secretary of the Army and other officials of the Office of the Secretary of the Army, in coordination with the AGC.

(2) Review for legal sufficiency requests submitted to the Office of the DCS, G–2 (ODCS, G-2) under the provisions of this regulation.

(3) Provide appropriate intelligence law and policy instruction.

(4) Review, in coordination with the Army General Counsel, all requests for exception, waiver, modification, or amendment of policies and procedures covered by this regulation.

d. The Deputy Chief of Staff, G–2 (DCS, G–2). The DCS, G–2 will—

(1) As the Army senior official of the intelligence community (IC), exercise Army staff responsibility for intelligence oversight and be responsible for the propriety of U.S. Army intelligence activities, under the provisions of AR 10–5.

(2) Implement DOD and higher policy, develop and write Army policy and procedures, and provide interpretation as required.

(3) Coordinate required DA- or higher level approvals.

(4) Ensure Federal crime reports, as described in chapter 16, are reported to the AGC and appropriate DOD officials.

(5) In incidents involving serious or continuing security breaches, recommend appropriate investigative or remedial actions, through the Secretary of the Army to DOD.

(6) Maintain appropriate Web pages for current policy interpretation, references, and training materials.

e. The Deputy Chief of Staff, G3/5/7 (DCS, G–3/5/7) and the Chief Information Officer, G–6 (CIO/G–6). The DCS, G–3/5/7 and the CIO/G–6 will—

(1) Refer to the DCS, G–2 any field requests it receives for approval of procedures described in this regulation.

(2) Include in operations policy the authorities and limitations on intelligence activities regarding U.S. person information.

f. The Provost Marshal General (PMG). The PMG will—

(1) Ensure that AR 190–40 includes a means to report Federal crimes directly to the AGC, as described in chapter 16.

(2) Include in appropriate law enforcement policy the authorities and limitations on intelligence activities regarding U.S. person information.

g. The Commander, U.S. Army Training and Doctrine Command (TRADOC). The Commander, TRADOC will—

(1) Develop intelligence oversight doctrinal literature and training programs, in close coordination with the DCS, G–2 (DCS, G–2)(DAMI–CDC) and the Commander, U.S. Army Intelligence and Security Command (INSCOM).

(2) Incorporate intelligence oversight training into resident and nonresident intelligence courses, all pre-command courses and all senior leadership courses.

(3) Ensure doctrine addresses the limitations on intelligence activities regarding U.S. persons, especially within the United States.

h. The Commanders, U.S. Army Central Command, Eighth U.S. Army, U.S. Army, Europe, U.S. Army Forces Command, U.S. Army Japan, U.S. Army Pacific, U.S. Army South, and U.S. Army Special Operations Command. These commanders will—

(1) Ensure, through the senior intelligence officer, the propriety of command intelligence activities.

(2) Approve, or delegate approval for, certain procedures as listed in this regulation for intelligence elements assigned or under the command's operational control that have an authorized function requiring use of those procedures.

(3) Ensure compliance with this regulation.

(4) Include the authorities and limitations on intelligence activities regarding U.S. persons in force protection plans and procedures.

(5) Notify INSCOM when INSCOM personnel will execute collection techniques under the command's operational control and approval.

(6) Include intelligence oversight in organizational inspection programs.

(7) Designate an intelligence professional in the intelligence operational chain as the organization intelligence oversight staff officer. Ensure the individual holds the appropriate security clearance and accesses, and has complete access to all information on command intelligence, intelligence support, and counterintelligence activities.

(8) Establish a review process to ensure U.S. person information was collected and retained in accordance with this regulation before transferring files to the Investigative Records Repository or information into intelligence databases.

(9) Establish a review process to ensure U.S. person information incorporated into intelligence databases is maintained in accordance with the Army Records Information Management System (ARIMS).

(10) Provide support, including legal advice, to 650th MI Group intelligence activities upon request.

i. The Commander, INSCOM. The Commander, INSCOM will—

(1) Have responsibility for the legality of INSCOM intelligence activities.

(2) Approve, or delegate approval authority for, certain procedures as listed in this regulation.

(3) Ensure compliance with this regulation.

(4) Include the authorities and limitations on intelligence activities regarding U.S. persons in force protection plans and procedures.

(5) Include intelligence oversight in organizational inspection programs.

(6) Designate an intelligence professional in the intelligence operational chain as the organization intelligence oversight staff officer. Ensure the individual holds the appropriate security clearance and accesses, and has complete access to all information on command intelligence, intelligence support, and counterintelligence activities.

(7) Establish a review process to ensure U.S. person information was collected and retained in accordance with this regulation before transferring files into the Investigative Records Repository or information into intelligence databases.

(8) Establish a review process to ensure U.S. person information incorporated into intelligence databases is maintained in accordance with ARIMS.

(9) Ensure that the Army Central Control Office reports the subjects of counterintelligence (CI) investigations whose activities also constitute a questionable intelligence activity, under the provisions of chapter 15, or a reportable Federal crime, under the provisions of chapter 16.

(10) Provide support, including legal advice, to 650th MI Group intelligence activities upon request.

j. The Commander, 650th MI Group. The Commander, 650th MI Group will—

(1) Be responsible for the legality of 650th MI Group intelligence activities.

(2) Approve, or delegate approval for, certain collection techniques as listed in this regulation.

(3) Ensure compliance with this regulation.

(4) Include the authorities and limitations on intelligence activities regarding U.S. persons in force protection plans and procedures.

(5) Include intelligence oversight in organizational inspection programs.

(6) Ensure requests for approval of 650th MI Group intelligence activities are reviewed by a U.S. legal advisor familiar with Army intelligence policy. The 650th may request this support from other Army commands.

(7) Designate an intelligence professional in the intelligence operational chain as the organization intelligence oversight staff officer. Ensure the individual holds the appropriate security clearance and accesses, and has complete access to all information on 650th activities.

(8) Establish a review process to ensure U.S. person information was collected and retained in accordance with this regulation before transferring files to the Investigative Records Repository or information into intelligence databases.

(9) Establish a review process to ensure U.S. person information incorporated into intelligence databases is maintained in accordance with ARIMS.

(10) Comply with North Atlantic Treaty Organization policies when they apply to requirements and responsibilities in this regulation.

k. The Chief, Army Reserve/Commander, Army Reserve Command. The Chief, Army Reserve/Commander, Army Reserve Command will—

(1) Ensure compliance with this regulation.

(2) Through the senior intelligence officer, ensure the propriety of intelligence activities.

(3) Include intelligence oversight in organizational inspection programs.

(4) Include the authorities and limitations on intelligence activities regarding U.S. persons in force protection plans and procedures.

(5) Ensure that questionable intelligence activity and Federal crimes reporting procedures exist within Army Reserve elements conducting foreign intelligence or counterintelligence activities.

(6) Designate an intelligence professional in the intelligence operational chain as the organization intelligence oversight staff officer. Ensure the individual holds the appropriate security clearance and accesses and has complete access to all information necessary to carry out responsibilities.

(7) Establish a review process to ensure U.S. person information was collected and retained in accordance with this regulation before transferring files to the Investigative Records Repository or information into intelligence databases.

(8) Establish a review process to ensure U.S. person information incorporated into intelligence databases is maintained in accordance with ARIMS.

l. The Chief, National Guard Bureau (NGB). The Chief, NGB will—

(1) Ensure compliance with this regulation.

(2) Establish intelligence oversight requirements and responsibilities within the Army National Guard (ARNG).

m. The Director, ARNG. The Director, ARNG will—

(1) Ensure that all ARNG personnel understand that military intelligence is exclusively a Federal mission.

(2) Ensure compliance with this regulation.

(3) Publish guidance to all State Adjutants General implementing an intelligence oversight program.

(4) Ensure State Adjutants General publish guidance for all subordinate commands, including all required training and reporting.

(5) Include the authorities and limitations on intelligence activities regarding U.S. persons in force protection plans and procedures.

(6) Appoint intelligence professionals as organizational intelligence oversight staff officers and ensure the individuals hold the appropriate security clearance and accesses and have complete access to all information necessary to carry out responsibilities.

(7) Establish a review process to ensure U.S. person information was collected and retained in accordance with this regulation before transferring information into intelligence databases.

(8) Establish a review process to ensure U.S. person information incorporated into intelligence databases is maintained in accordance with ARIMS.

n. The State Adjutants General. On the basis of ARNG guidance, the State Adjutants General will—

(1) Publish intelligence oversight program guidance for all subordinate commands and ensure compliance with this regulation.

(2) At a minimum, appoint an intelligence professional, at the State Area Command level, to be the State intelligence oversight staff officer, and ensure that all intelligence components within the State have an intelligence oversight staff officer down to battalion level in MI units and brigade level in all other units.

(3) Accomplish intelligence oversight inspections as required in this regulation and AR 20–1.

(4) Ensure reports of questionable intelligence activities are forwarded to the NGB Inspector General (IG).

o. Army IGs. Army IGs will—

(1) As part of their inspection program, determine if intelligence elements are conducting foreign intelligence and counterintelligence activities in compliance with this and other applicable regulations.

(2) Ascertain whether any organization, staff, or office not specifically identified as an Army intelligence element is being used for foreign intelligence or counterintelligence purposes and, if so, ensure its activities comply with this regulation.

(3) Evaluate leadership awareness and understanding of the authorities for intelligence collection of U.S. person information.

(4) Ensure that procedures exist within each element for reporting questionable intelligence activities, and that personnel are aware of their reporting responsibility.

(5) Provide advice to the commander and intelligence oversight staff officer as needed.

(6) Per TIG (SAIG–IO) guidance, describe significant intelligence oversight activities and inspections and suggestions for improvement in the program for the TIG (SAIG–IO) quarterly report to ATSD–IO.

p. Commanders of units with military intelligence missions. These commanders will—

(1) Ensure all assigned or attached personnel conducting intelligence activities do so in accordance with U.S. law and policy.

(2) Ensure MI personnel and non-MI personnel conducting intelligence activities, are fully aware of and comply with their individual responsibilities as outlined in this regulation.

(3) Ensure unit personnel and supporting contractors receive the training described in paragraph 14–1, as a routine part of unit training programs.

(4) Designate an intelligence professional in the intelligence operational chain to function as the organization intelligence oversight staff officer who holds the appropriate security clearance and accesses and who has complete access to all information necessary to carry out responsibilities.

(5) Implement a review process to ensure U.S. person information was collected and retained in accordance with this regulation before transferring files to the Investigative Records Repository or information into intelligence databases.

(6) Implement a review process to ensure U.S. person information incorporated into intelligence databases is maintained in accordance with ARIMS.

1–5. Limitations and restrictions

a. This regulation does not itself authorize intelligence activity. An Army element must first have the mission and authority to conduct the intelligence activity. This is assigned by other regulations.

b. This regulation does not apply to Army intelligence components when engaged in civil disturbance or law enforcement activities. Army intelligence components engaged in civil disturbance activities will do so in accordance with civil disturbance plan GARDEN PLOT. When intelligence collection, an investigation, or inquiry undertaken pursuant to this regulation establishes a reasonable belief that a crime has been committed, the Army intelligence component concerned will refer the matter to the appropriate law enforcement agency in accordance with procedure 12 and chapter 16, or if the Army intelligence component is otherwise authorized to conduct law enforcement activities, will conduct that investigation under appropriate law enforcement procedures.

c. Nothing in this regulation is intended to authorize any US Army intelligence component to conduct activities or obtain approvals for activities that would not be in accordance with the procedures established in DOD 5240.1-R, if applicable. Where the language used in this regulation differs from that used in a corresponding provision of DOD 5240.1-R, the language in DOD 5240.1-R controls.

d. The fact that a collection category exists does not convey authorization to collect. There must be a link between

the U.S. person information to be collected and the element's assigned mission and function. This link is particularly important in open source intelligence and data exploitation.

e. MI personnel will not participate in or request any person or agency to undertake activities forbidden by Executive Order (EO) 12333, as amended by EOs 13284 and 13355.

f. No MI personnel will engage in, or conspire to engage in, assassination.

g. MI elements are prohibited from conducting or providing support to special activities (see glossary) unless approved by the President and directed by the Secretary of Defense in time of congressionally declared war, or during a period covered by a presidential report/finding and as the Secretary of Defense directs.

1–6. Legal advice, conflicts with other policy, and understanding terminology

a. Commanders will seek legal advice from their supporting U.S. legal advisor. The legal advisor must review all activities to be conducted pursuant to chapters 5 through 13.

b. When questions cannot be resolved locally, they will be forwarded through command channels for resolution.

c. If provisions in this regulation conflict with new or revised DOD policy, DOD policy takes precedence.

d. Note that this document uses terms that differ considerably from standard Army usage. The reader must be thoroughly familiar with the glossary in order to understand this regulation.

1–7. Records management

a. Unless otherwise specified, those approval authorities defined in this regulation will forward to the DCS, G–2 (DAMI–CDC) information copies of plans, concepts or orders approved pursuant to procedures 5 through 11. All approval authorities in this regulation will forward the original signature approval document(s) to the element maintaining the record dossier or file.

b. When an office maintaining a questionable intelligence activity file is not the actual investigating agency or an oversight office, it will file these reports under an appropriate general correspondence file number.

c. When the command conducts an investigation under the provisions of AR 15–6 on activities reported per chapter 15, the report is filed under File Number (FN) 15–6b.

d. Investigative agencies, such as law enforcement, inspectors general, and counterintelligence, will file the actual inquiry or investigation under appropriate investigative FN. Intelligence oversight officials may provide copies of documents they produce to the investigating agency for inclusion in the investigative record dossier.

e. Federal crime reports (chapter 16) will be filed under FN 190–40a or general correspondence, as appropriate.

f. FN 381–10a, Technical Surveillance Index, will apply only to the U.S. Army Investigative Records Repository.

1–8. Presumptions

a. A person or organization outside the United States is presumed not to be a U.S. person, unless the intelligence component obtains specific information to the contrary.

b. An alien in the United States is presumed not to be a U.S. person, unless the intelligence component obtains specific information to the contrary.

1–9. Internet considerations

a. MI elements must use Government computers to access the internet for official Government business unless otherwise authorized.

b. If operational security so requires, such as to protect a Government computer from hacker retaliation, Commanders, INSCOM and 650th MI Group may approve nonattributable internet access. See current DCS, G–2 memoranda for guidance.

c. Internet protocol (IP) addresses, uniform resource locators (URLs), and e-mail addresses that are not self-evidently associated with a U.S. person may be acquired, retained, and processed by Army intelligence components without making an effort to determine whether they are associated with a U.S. person as long as the component does not engage in analysis focused upon specific addresses. Once such analysis is initiated, the Army intelligence component must make a reasonable and diligent inquiry to determine whether the data are associated with a U.S. person.

Chapter 2
Procedure 2: Collecting U.S. Person Information

2–1. General

This chapter specifies the kinds of U.S. person information that MI may collect and the general means by which the information may be collected.

2–2. Types of collectable information

MI may collect U.S. person information only when it is necessary to fulfill an assigned function and when it falls within one of the following categories:

a. Consensual—The U.S. person consents to MI collecting information about him or her.

b. Publicly available information—the U.S. person information is publicly available.

c. Foreign intelligence—U.S. person information in this category is limited to—

(1) Individuals reasonably believed to be officers or employees, or otherwise acting for or on behalf of, a foreign power.

(2) An organization reasonably believed to be owned or directly or indirectly controlled by a foreign power.

(3) Individuals or organizations reasonably believed to be engaged or about to engage in international terrorist or international narcotics activities.

(4) Individuals reasonably believed to be prisoners of war, missing in action, or the targets, hostages, or victims of international terrorist organizations.

(5) Corporations or other commercial organizations believed to have some relationship with foreign powers, organizations or persons.

d. Counterintelligence—U.S. person information in this category is limited to—

(1) Individuals reasonably believed to be engaged in, or about to engage in, activities that are within Army CI investigative jurisdiction, including intelligence activities on behalf of a foreign power or international terrorist activities.

(2) Individuals in contact with those described in paragraph 2–2*d*(1), so that MI may identify the individuals and assess their relationship.

e. Potential sources of assistance—U.S. persons reasonably believed to be potential intelligence sources, or potential sources of assistance to intelligence activities, so that MI may assess their suitability or credibility.

f. Protecting intelligence sources and methods—Information about a U.S. person who has/had access to or possession of information revealing foreign intelligence and counterintelligence sources or methods, when the collection is necessary to protect against the unauthorized disclosure of that information. Within the United States, collection is limited to—

(1) Present and former DOD employees.

(2) Present or former employees of a current or former DOD contractor.

(3) Employment applicants to DOD or a DOD contractor.

g. Physical security—Information concerning a U.S. person who is reasonably believed to threaten the physical security of DOD employees, installations, operations or official visitors (see AR 190–13 and AR 525–13).

h. Personnel security—U.S. person information developed from a lawful personnel security investigation. This applies only to those MI elements authorized to conduct personnel security investigations in support of the Defense Security Service or Office of Personnel Management (see AR 380–67).

i. Communications security—U.S. person information developed during a lawful communications security inquiry or investigation. (see AR 380–53)

j. Narcotics—Information about a U.S. person who is reasonably believed to be engaged in international narcotics activities.

k. Threats to safety—U.S. person information that is required to protect the safety of any person or organization, including those who are targets, victims, or hostages of international terrorist organizations (see AR 525–13).

l. Overhead reconnaissance—Information from overhead reconnaissance not directed at specific U.S. persons.

m. Administrative purposes—U.S. person information necessary for administrative purposes.

2–3. General collection means

MI may collect U.S. person information by any lawful means but must exhaust the least intrusive collection means before requesting a more intrusive collection means. In general, this means—

a. Collection is made first from publicly available sources or with the U.S. person's consent.

b. If that collection is not feasible or sufficient, MI will seek to collect the U.S. person information from cooperating sources.

c. If cooperating source information is not feasible or sufficient, MI will seek to collect using other lawful means are used that do not require a warrant or Attorney General approval.

d. If none of the above means is feasible, MI units may request approval for the use of techniques requiring a warrant or Attorney General approval.

2–4. Limitation on foreign intelligence collection within the United States

Within the United States, foreign intelligence concerning U.S. persons may be collected only by overt means, unless all the following conditions are met:

a. The foreign intelligence sought is significant and does not concern a U.S. person's domestic activities.

b. The foreign intelligence cannot be reasonably obtained by overt means.

c. Collection has been coordinated with the Federal Bureau of Investigation (FBI).

d. Other than overt means was approved in writing by the DCS, G–2 or the Commander, INSCOM.

2–5. First Amendment protection

Nothing in this procedure will be interpreted as authorizing the collection of any information relating to a U.S. person solely because of that person's lawful advocacy of measures opposed to Government policy.

Chapter 3
Procedure 3: Retaining U.S. Person Information

3–1. General

This chapter describes the kinds of U.S. person information that may be knowingly retained without the individual's consent.

3–2. Retention criteria

Retention is authorized under the following criteria:

a. Information properly collected in accordance with chapter 2.

b. Information acquired incidentally. The information was acquired incident to an otherwise authorized collection, and may be retained if the information—

(1) Could have been collected intentionally under the provisions of chapter 2.

(2) Is necessary to understand or assess foreign intelligence or counterintelligence.

(3) Is foreign intelligence or counterintelligence collected from authorized electronic surveillance.

(4) Is incidental to authorized collection and may indicate involvement in activities that may violate Federal, State, local, or foreign law.

c. Information relating to functions of other Army activities, DOD components, or non-DOD agencies. The information pertains solely to the functions and responsibilities of other activities, components or agencies, and is retained only as necessary to transmit the information to that agency. The transmittal is filed and destroyed under general correspondence records management. The information will not be retained in MI databases or repositories.

d. Temporary retention. Information may be retained up to 90 days, solely to determine if the information is, in fact, retainable under this regulation. The 90-day period starts upon receipt of the information.

e. Other information. Information not covered in this chapter will be retained only to report the collection for oversight purposes and for necessary subsequent proceedings.

3–3. Access and retention duration

a. Access controls. Access to U.S. person information retained in intelligence files, databases and repositories is limited to those with a need to know the information.

b. Retention duration. U.S. person information in intelligence files, databases, and repositories is retained in accordance with disposition criteria in AR 25–400–2. U.S. person information deleted from user electronic files, but remaining on servers or archived files, may remain until systems administrators purge or retire them in accordance with systems maintenance policies, AR 25–400–2, or Archivist of the United States disposition instructions.

c. Annual review. Intelligence components will review intelligence files and databases annually. Intelligence components will specifically review US person information to ensure its retention is still necessary to an assigned function. This ensures U.S. person information is not held beyond established disposition criteria, is retained for an authorized function, and was not retained in violation of this regulation. The review may be conducted in increments, as long as all holdings are reviewed annually. This does not apply to the Investigative Records Repository or other authorized long-term records holding areas.

Chapter 4
Procedure 4: Disseminating U.S. Person Information

4–1. General

This chapter governs the types of information regarding U.S. persons that may be disseminated, without the person's consent, outside of the Army intelligence component which collected and retained the information. It does not apply to

information collected solely for administrative purposes; disseminated pursuant to law; or disseminated pursuant to a court order that imposes dissemination controls.

4–2. Dissemination criteria

Nonsignals intelligence information about a U.S. person may be disseminated without that person's consent under the following conditions:

a. The information was collected or retained under provisions 2 and 3.

b. The recipient is reasonably believed to have a need for the information to fulfill a lawful assigned governmental function and is—

(1) A DOD employee or a DOD contractor employee.

(2) A Federal, State, or local law enforcement entity when the information is in the recipient's jurisdiction.

(3) An agency of the U.S. IC so that it can determine if the information is relevant to agency responsibilities.

(4) A non-DOD or non-IC Federal agency.

(5) A foreign government, under the provisions of existing policy, agreements, and other understandings with the United States (see AR 380–10).

c. Dissemination outside DOD of information about a U.S. citizen or permanent resident alien from a U.S. Army system of records requires disclosure accounting under the provisions of AR 340–21.

d. Any dissemination that does not conform to the conditions set forth in paragraphs 4–1, 4–2*a*, and 4–2*b* must be approved by the legal office responsible for advising the DOD component concerned after consultation with the Department of Justice and DOD General Counsel. Such a determination will be based on a conclusion that the proposed dissemination complies with applicable laws, executive orders, and regulation. Requests will be forwarded through command channels to the ODCS, G–2 (DAMI–CDC).

4–3. Other dissemination

The AGC approves any other dissemination not conforming to paragraph 4–2 in coordination with the DOD General Counsel and the Department of Justice. These dissemination requests are forwarded through command channels to the ODCS, G–2 (DAMI–CDC).

Chapter 5
Procedure 5: Electronic surveillance

This chapter implements the Foreign Intelligence Surveillance Act (FISA) of 1978 (Title 50, United States Code, section 1805) (50 USC 1805).

Section I
Electronic Surveillance Within the United States

Army CI may conduct electronic surveillance against persons within the United States pursuant to an order issued by the Foreign Intelligence Surveillance Court (FISC) or upon Attorney General authorization.

5–1. Approvals

Forward requests for FISC orders or Attorney General authorization through command channels to the ODCS, G–2 (DAMI–CDC), which will seek Secretary of the Army approval, then send through DOD General Counsel to the Attorney General.

5–2. Emergency surveillance

a. Army CI may conduct emergency electronic surveillance within the United States upon Attorney General approval, in accordance with FISA.

b. Forward the request to the ODCS, G–2 (DAMI–CDC).

5–3. Documenting the surveillance request

Each request (also known as a statement of finding) must include—

a. Who or what is the target of the surveillance (for example, e-mail address, IP address, URL, or named individual or organization).

b. Location of the target of the surveillance.

c. The device/medium being targeted (for example, cellular telephone, cordless telephone, e-mail, internet chat rooms, bulletin board systems, Internet service provider server, facsimile machines).

d. How the medium will be targeted.

e. From where the surveillance is being conducted.

f. If applicable, the physical and/or electronic address(es); service provider identification, warning notices, user

agreements, command communications policies, and command security policies and practices; telephone number; room number; whether on public or private property; and any other relevant information.

g. A factual summary showing probable cause to believe the target is under at least one of the following categories:

(1) Engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, international terrorist activities, activities in preparation for international terrorist activities, or conspiring with or knowingly aiding and abetting a person engaging in such activities, for or on behalf of a foreign power.

(2) An officer or employee of a foreign power.

(3) Knowingly taking direction from or acting in knowing concert with, and thereby unlawfully acting for or at the direction of a foreign power.

(4) A corporation or other entity that is owned or controlled directly or indirectly by a foreign power.

(5) In contact with, or acting in collaboration with, a foreign intelligence or security service, to provide access to information or material classified by the United States and to which the subject has gained access.

h. A factual summary showing that the significant foreign intelligence or counterintelligence expected to be intercepted cannot be gathered by less intrusive means.

i. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the surveillance.

j. A description of the means by which the electronic surveillance will be conducted, including the equipment, recording device, and installation means.

k. If trespass is required to install the surveillance means, a statement supporting a finding that the means involve the least amount of intrusion necessary for installation.

l. The surveillance time period, not to exceed 90 days.

m. A description of why less-intrusive means are inappropriate.

n. If known, a description of all previous electronic surveillance on any of the same persons.

o. If requesting an extension of existing electronic surveillance, a description of results to date or an explanation of the failure to obtain results.

p. The expected dissemination of the surveillance product, including the procedures governing retention and dissemination of incidentally acquired U.S. person information.

Section II
Electronic Surveillance Outside the United States

This section applies to electronic surveillance outside the United States of persons who have a reasonable expectation of privacy.

5–4. Approvals of U.S. person surveillance

MI may conduct electronic surveillance against a U.S. person outside the United States only after Attorney General approval. Forward requests through command channels to the ODCS, G–2 (DAMI–CDC), which will staff the request for Secretary of the Army signature, through DOD General Counsel to the Attorney General (see para 5–3 for required documentation).

5–5. Emergency surveillance of U.S. persons

a. MI may conduct emergency surveillance of a U.S. person outside the United States without prior Attorney General approval if—

(1) The time required for Attorney General approval would cause failure or delay in obtaining significant foreign intelligence or counterintelligence, and that failure or delay would result in substantial harm to the national security.

(2) A person's life or physical safety is reasonably believed to be in immediate danger.

(3) The physical security of a DOD installation or other Government property is reasonably believed to be in immediate danger.

b. Emergency electronic surveillance approval authorities are the Secretary of the Army or Under Secretary of the Army, or any U.S. general/flag officer in the following positions:

(1) Commander, U.S. Army Forces Central Command.

(2) Commander, Eighth U.S. Army.

(3) Commander, U.S. Army Europe.

(4) Commander, U.S. Army Intelligence and Security Command.

(5) Commander, U.S. Army Pacific.

(6) Commander, U.S. Army South.

(7) Commander, U.S. Army Special Operations Command.

(8) Supreme Allied Commander Europe or designee for the 650th MI Group.

(9) Any other U.S. general/flag officer at the overseas location who has responsibility for either the surveillance target or for the endangered persons, installations, or materiel.

c. The approving authority must coordinate with the command's senior intelligence officer and staff judge advocate before approval.

d. The approving authority must notify the ODCS, G–2 (DAMI–CDC) by the most expeditious means available of the surveillance, the circumstances surrounding its authorization, the results to date, and any other information necessary to authorize continuation. The DCS, G–2 (DAMI–CDC) will notify AGC and the Secretary of the Army for passage through the DOD General Counsel to the Attorney General.

e. The emergency surveillance may not continue longer than 72 hours or until the Attorney General approves the surveillance, whichever is shorter.

5–6. Electronic surveillance of non-U.S. persons abroad

Electronic surveillance of non-U.S. persons abroad may be approved for any function assigned to an Army intelligence component.

a. Each request will—

(1) Provide information sufficient to show a reasonable belief that the surveillance will gather valuable intelligence information.

(2) Describe the nature and content of communications to be intercepted.

(3) Identify any U.S. persons whose communications could reasonably be expected to be intercepted.

(4) Describe the means by which the electronic surveillance will be conducted, including the equipment, recording device, and installation means.

b. Initial approvals and renewal requests may be granted for up to 120 days. Renewal requests for electronic surveillance of a continuing and long-term interest may be approved for up to 1 year.

c. Approval authorities are those officials listed in paragraph 5–5*b*(1) through (9) who may delegate approval authority, in writing, to deputy commanders, chiefs of staff, senior intelligence officers, corps commanders, division commanders, or the responsible MI brigade or group commander. No further delegation is authorized.

5–7. Inadvertent interception of U.S. person information

If a U.S. person communication is inadvertently intercepted during an electronic surveillance approved under para 5–6, the following applies:

a. If the U.S. person information is of foreign intelligence or counterintelligence value, the Army intelligence component conducting surveillance will request approval from the AGC, through the DCS, G–2, to retain and disseminate the information.

b. MI will not target the U.S. person for additional electronic surveillance until approved under the provisions of paragraph 5–4.

Section III
Signal Intelligence, Technical Surveillance Countermeasures, and Vulnerability and Hearability Surveys

This section applies to Army elements with signal intelligence, TSCM, and signal analysis missions and functions.

5–8. Signal intelligence and information systems security monitoring

a. MI elements conducting signal intelligence will comply with relevant National Security Agency/Central Security Service directives, which takes precedence over this regulation for signal intelligence missions.

b. MI elements conducting information systems security monitoring will comply with AR 380–53.

5–9. Technical surveillance countermeasures

This paragraph implements FISA (50 USC 1805). MI may use TSCM that involve incidental acquisition of U.S. person nonpublic communications when—

a. The official in charge of the facility, organization, or installation has requested or consented to a TSCM service.

b. TSCM are limited to the time necessary to determine the existence and capability of unauthorized electronic surveillance activities or equipment.

c. Access to acquired communications is limited to the TSCM personnel directly involved, and the content is destroyed as soon as practical or upon completion of the service, except as follows:

(1) If acquired in the United States, information may be retained and disseminated as necessary to protect against unauthorized electronic surveillance or to enforce 18 USC Chapter 119, and the Communication Act of 1934, 47 USC 605.

(2) If acquired outside the United States, information that indicates a violation of Federal law, or a clear and imminent threat to life or property, may also be disseminated to appropriate law enforcement authorities.

(3) TSCM elements may retain a record of the types of communications and information subject to acquisition by the illegal electronic surveillance.

d. TSCM elements will comply with policy requirements on use, retention, or dissemination of U.S. person information acquired during TSCM activities.

5–10. Vulnerability and hearability surveys

MI will conduct vulnerability or hearability surveys, as defined in the glossary, in accordance with AR 380–53.

Section IV
Developing, Testing, and Calibrating Electronic Equipment

This section applies to developing, testing, or calibrating electronic equipment that can intercept or process communications and noncommunications signals. It includes research and development that needs electronic communications as a signal source.

5–11. Authorized use

a. The following signals may be used without restriction:

(1) Laboratory-generated signals.

(2) Communications signals with the communicator's consent.

(3) Commercial or public service broadcast band communications.

(4) Communications transmitted between terminals outside the United States, not used by any known U.S. person.

(5) Noncommunications signals, including telemetry and radar.

b. Communications subject to lawful electronic surveillance, as described in this chapter, may be used subject to applicable minimization procedures.

c. The following may be used subject to the restrictions of paragraph 5–12:

(1) Communications over official Government communications circuits, with consent from an appropriate official of the controlling agency.

(2) Communication in citizens and amateur radio bands.

d. Other signals, when it is not practical to use the signals described above and not reasonable to obtain the consent of U.S. persons incidentally subjected to the surveillance. In addition to the restrictions of paragraph 5–12—

(1) When the period of use exceeds 90 days, the Attorney General must approve the use.

(2) The using element will submit a test proposal to the ODCS, G–2 (DAMI–CDC), for processing through the AGC and DOD General Counsel to the Attorney General.

(3) The test proposal will include the nature of the activity, the organization that will conduct the activity, the reasons why the test must exceed 90 days, and the proposed disposition of any signals or communications acquired.

5–12. Restrictions

For signals described in paragraphs 5–11*c* and *d*, these restrictions apply:

a. Organizations will limit the surveillance scope and duration to meet the needs described in paragraph 5–11.

b. Organizations will not intentionally target a particular U.S. person without consent.

c. The communications content will be—

(1) Retained only when actually needed for the purposes described in this section.

(2) Disseminated only to personnel conducting the activity.

(3) Destroyed immediately upon activity completion.

d. The technical parameters (such as frequency, modulation, bearing, signal strength, and time of activity) may be retained and used as stated in paragraph 5–11, or for collection avoidance. The parameters may be disseminated to DOD intelligence components and other entities authorized to conduct electronic surveillance or related development, testing, and calibration.

Section V
Electronic Communications and Surveillance Equipment Training

This section applies to training personnel in the operation and use of electronic communications and surveillance equipment. It does not apply to consensual communications surveillance or to nonintelligence components that train intelligence personnel.

5–13. Training guidance

Training must include instruction about the requirements and restrictions of the FISA and EO 12333, as amended by EOs 13284 and 13355, concerning the unauthorized acquisition and use of the content of U.S. person communications and guidance on the authorized use (para 5–11) and restrictions (para 5–12).

5–14. Limitations

a. Except as permitted by paragraph 5–14*c*, using electronic communications and surveillance equipment for training is permitted subject to the following limitations:

(1) To the maximum extent practicable, all equipment will be focused against communications that are subject to lawful electronic surveillance for foreign intelligence and counterintelligence purposes under sections I, II, and III of this chapter.

(2) Organizations will not aurally acquire the contents of a private communication of a nonconsenting U.S. person unless the person is an authorized electronic surveillance target.

(3) The extent and duration of electronic surveillance will be limited to that necessary to train personnel in equipment use.

b. Public and Government signals may be used for training as follows:

(1) Public broadcasts, distress signals, or official U.S. Government communications may be monitored.

(2) When Government agency communications are monitored, obtain an appropriate official's consent.

(3) Minimal acquisition of information is permitted as required for calibration.

c. Information collected from communications described in paragraph 5–14*a*(1) will be retained and disseminated in accordance with minimization procedures applicable to that electronic surveillance.

d. Other information collected during training, or that is acquired incidentally, will be destroyed as soon as practical or upon training completion and will not be disseminated for any purpose. This does not apply to distress signals.

Section VI
Consensual Communications Intercepts

MI may conduct consensual communications intercepts for any assigned lawful function. One or more, but fewer than all, parties to the communication must consent for the intercept to be considered consensual.

5–15. Documentation requirements

Consensual intercept documentation must include—

a. A description of the MI lawful function requiring the intercept.

b. Who or what is the target of the intercept (for example, e-mail address, IP address, URL, or named individual or organization).

c. Location of the target of the intercept.

d. What is the device/medium being targeted (for example, cellular telephone, cordless telephone, e-mail, internet chat rooms, bulletin board systems, ISP server, or facsimile machines).

e. How is the medium being targeted (for example, trap and trace device, pen register, sniffer program, or keystroke monitoring).

f. From where is the intercept being conducted.

g. Description of the circumstances requiring the intercept, the means by which it will occur, and the expected duration.

h. Name or description (if name unknown) of the individuals whose communications are to be intercepted, and their roles (for example, case officer, source, foreign agent, investigator, witness, or subject).

i. When practical, written consent of at least one party to the communications, and preferably as many participants as possible.

5–16. Approvals

a. When conducted within the United States, or against a U.S. person outside the United States, requests are forwarded to the DCS, G–2 (DAMI–CDC) for Secretary of the Army, Under Secretary of the Army, or AGC approval.

b. When directed against a non-U.S. person outside the United States, these officials may approve the intercept. The officials below may delegate, in writing, approval authority as necessary, to deputy commanders, chiefs of staff, senior intelligence officers, corps commanders, division commanders, or the responsible MI brigade or group commander:

(1) DCS, G–2.

(2) Commander, U.S. Army Forces Central Command.

(3) Commander, Eighth U.S. Army.

(4) Commander, U.S. Army Europe.

(5) Commander, INSCOM.

(6) Commander, U.S. Army Pacific.

(7) Commander, U.S. Army South.

(8) Commander, U.S. Army Special Operations Command.

(9) Supreme Allied Commander, Europe.

(10) Commander, 650th MI Group.

c. In an emergency, an MI element may conduct consensual intercepts in the conduct of Army CI investigations and operations within the United States, or directed against U.S. persons outside the United States, when—

(1) Approved by a general court-martial convening authority, and prior Secretary of the Army, Under Secretary of the Army, or AGC approval is not practical because—

(a) Time required would cause failure or delay in obtaining valuable information.

(b) A person's life or physical safety is reasonably believed to be in immediate danger.

(c) Physical security of a DOD facility or Government property is reasonably believed to be in immediate danger.

(2) The DCS, G–2 (DAMI–CDC) is notified within 24 hours of the surveillance, the reason for authorizing it, the expected results, and the documentation for DCS, G–2 approval. The emergency surveillance may continue until the DCS, G–2 advises formal approval is granted, or approval is denied. If approved, the surveillance may continue under normal procedures. If denied, the element conducting surveillance will cease immediately, and the collected information will be reviewed for retention under Procedures 2 and 3, or pursuant to guidance provided in the notification of denial.

Section VII
Exceptions

The following activities are exempt from the requirements of Procedure 5, provided they are conducted with the stipulations specified below.

5–17. Computer trespasser intecepts

Under 18 USC 2511(2)(i), the electronic communications of a computer trespasser transmitted to, through, or from a protected computer may be intercepted by Army CI elements under the following circumstances:

a. The owner or operator of a protected computer authorizes, in writing, the interception of the computer trespasser's communications on the protected computer.

b. The interception is to be conducted pursuant to a lawful Army CI investigation.

c. The Army CI Agent proposing the interception has reason to believe that the contents of the computer trespasser's communication will be relevant to the investigation.

d. The interception does not acquire communications other than those transmitted to or from the computer trespasser.

5–18. Approvals

a. The following officials may approve interceptions of a computer trespasser's communications on a protected computer for 90-day periods, subsequent to a legal review that has been documented in writing, for any proposed intercept which specifically addresses the required conditions/criteria in 5–17*a* through *d*:

(1) DCS, G–2.

(2) Army G–2X.

(3) Commander, INSCOM.

(4) Commander, 650th MI Group.

b. Within 48 hours of approval, the approving official will forward the approval documentation, along with the corresponding written legal review, to the Army General Counsel.

Chapter 6
Procedure 6: Concealed Monitoring

6–1. Scope

This chapter applies to concealed monitoring only for foreign intelligence and counterintelligence purposes conducted within the United States or directed against a U.S. person outside the United States, where the subject does not have a reasonable expectation of privacy and where no warrant would be required if the monitoring was undertaken for law enforcement purposes.

a. Within the United States, when the subject has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, concealed monitoring will be treated and processed as electronic surveillance (see chap 5, sec I). Monitoring is considered within the United States if the monitoring device, or the monitored target, is located within the United States.

b. When a U.S. person outside the United States has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, concealed monitoring will be treated and processed as electronic surveillance of a U.S. person outside the United States (see chap 5, sec III).

c. When a non-U.S. person outside the United States has a reasonable expectation of privacy, concealed monitoring will be treated and processed as electronic surveillance of a non-U.S. person outside the United States (see para 5–6).

d. Beacons (beepers) and transponders are considered concealed monitoring when—

(1) Affixed in a public place, such as on a vehicle in a public parking lot.

(2) No warrant would be required for law enforcement purposes.

(3) The monitoring stops when the target acquires an expectation of privacy, such as driving the vehicle into his home garage.

6–2. Key considerations

a. When determining if concealed monitoring is appropriate, the following will be examined:

(1) Purpose: The monitoring is necessary for assigned foreign intelligence or counterintelligence functions and does not constitute electronic surveillance under chapter 5, sections I or II.

(2) Definition: Concealed monitoring is the targeting, by electronic, optical, or mechanical means, the movements and activity of an individual or group.

(3) Electronic means: Includes transponders, beepers, Global Positioning System locators and other electronic means of observing or tracking people.

(4) Optical means: Includes cameras and lenses of any type.

(5) Mechanical means: Devices that are not electronic or optical.

b. Because the same or similar techniques are often used for electronic surveillance, careful review is necessary during the approval process to ensure that procedure 5 does not apply.

6–3. Limitations

Concealed monitoring is limited to—

a. Use on a DOD-owned or -leased installation or facility within the United States.

b. Outside a DOD-owned or -leased installation or facility within the United States pursuant to a counterintelligence investigation conducted under the provisions of AR 381–20. Such activity will be coordinated with the FBI.

c. Use on DOD-owned or -leased installations or facilities outside the United States. Monitoring outside these facilities may be conducted after coordination with the Central Intelligence Agency (CIA) and host nation officials if required under Status of Forces Agreements (SOFA).

6–4. Approvals

The DCS, G–2 and Commander, INSCOM may approve concealed monitoring based on a determination that such monitoring is necessary to conduct an assigned foreign intelligence or CI function and does not constitute electronic surveillance. No other approving officials are currently authorized.

Chapter 7
Procedure 7: Physical Searches

7–1. Nonconsensual searches within the United States

a. Army counterintelligence elements are authorized to conduct nonconsensual physical searches of active duty military personnel or their property within the United States when—

(1) Authorized by a military judge or a designated military magistrate.

(2) Authorized by a military commander empowered to approve physical searches for law enforcement purposes under the provisions of the Manual for Courts Martial.

(3) There is probable cause to believe that the subject is acting as an agent of foreign powers.

b. MI will ask the FBI to conduct any other nonconsensual search for foreign intelligence or counterintelligence purposes (see para 7–6).

7–2. Nonconsensual searches of United States persons outside the United States

a. Army counterintelligence elements are authorized to conduct nonconsensual physical searches of active duty military personnel or their property outside the United States when—

(1) Authorized by a military judge or a designated military magistrate.

(2) Authorized by a military commander empowered to approve physical searches for law enforcement purposes under the provisions of the Manual for Courts Martial.

(3) There is probable cause to believe that the subject is acting as an agent of a foreign power.

b. MI may conduct other nonconsensual physical searches of U.S. persons for foreign intelligence or CI purposes with approval of the Attorney General as specified in paragraph 7–5a.

7–3. Documenting the request

Requests for approval to conduct nonconsensual physical searches must include—

a. Identification of the person or description of the property to be searched.

b. A statement of facts to show there is probable cause to believe the subject of the search is—

(1) Engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, international terrorist activities, activities in preparation for international terrorist activities, or conspiring with or knowingly aiding and abetting a person engaging in such activities, for or on behalf of a foreign power.

(2) An officer or employee of a foreign power.

(3) Knowingly taking direction from or acting in knowing concert with, and thereby unlawfully acting for or at the direction of a foreign power.

(4) A corporation or other entity that is owned or controlled directly or indirectly by a foreign power.

(5) In contact with, or acting in collaboration with, a foreign intelligence or security service, to provide access to information or material classified by the United States and to which the subject has access.

c. A statement of facts to show that the significant foreign intelligence or counterintelligence expected to be obtained cannot be gathered by less intrusive means.

d. A description of the significant foreign intelligence or counterintelligence expected to be obtained from the search.

e. A description of the extent of the search and a statement of facts to show that the search will involve the least amount of physical intrusion to meet the objective.

f. A description of the expected dissemination of the product of the search, including the procedures governing the retention and dissemination of incidentally acquired U.S. person information.

7–4. Nonconsensual searches of non-U.S. persons outside the United States

a. Army counterintelligence elements may conduct nonconsensual physical searches of the property of non-U.S. persons outside the United States pursuant to a lawful CI function and subsequent to a legal review by the supporting U.S. legal advisor.

b. Each request will—

(1) Include information sufficient to show a reasonable belief that the search will yield significant foreign intelligence or counterintelligence information.

(2) Describe the property to be searched and its location.

(3) Describe the means by which the search will be conducted.

7–5. Approvals

a. Requests for approval of physical searches identified in paragraphs 7–1*b* and 7–2*b* will be forwarded through command channels to the DCS, G–2 (DAMI–CDC). The DCS, G–2 will seek Secretary of the Army or Under Secretary of the Army approval, then rout the request through the DOD General Counsel for Deputy Secretary of Defense review before transmission to the Attorney General.

b. Original approval authority for the conduct of those physical searches identified in paragraph 7–4 rests with the DCS, G–2, who may further delegate this authority to the Army G–2X and Commanders, INSCOM and 650th MI Group. No further delegation of this authority is authorized.

7–6. Military intelligence assistance to Federal Bureau of Investigation surreptitious entry and physical search

a. Paragraph 7–1 notwithstanding, the Department of Justice, DOD, and CI policy will authorize CI assistance to the FBI in support of Army CI investigations for which DOD is not assigned investigative responsibility and encourage cooperation between DOD CI elements and the FBI.

b. To that end, the Commander, INSCOM may authorize CI technical assistance in FBI surreptitious entries and physical searches in the United States, under the following circumstances:

(1) The FBI will provide a written request for such assistance.

(2) The Commander or Deputy Commander, INSCOM will approve the requested support.

(3) The requested support will be authorized by an FBI obtained FISC order. When the assistance is to occur outside a military installation, the FISC order must name the Army or DOD as a specified person and direct the necessary support;

(4) The FBI will provide onsite supervision of the surreptitious entry and physical search.

(5) INSCOM concurrently will provide a copy of the FBI request, FISC order, and INSCOM approval to the ODCS, G–2 (DAMI–CDC) for review. The approval will be provided to the ODCS, G–2 (DAMI–CDC) in advance of the activity whenever possible.

c. FBI requests for Army CI support of surreptitious entries and physical searches that either do not meet the above

criteria or raise additional issues will be forwarded to the ODCS, G–2 (DAMI–CDC) for determination of appropriate approval authority.

Chapter 8
Procedure 8: Mail Searches and Examination

8–1. General

a. This chapter applies to mail covers and the opening of mail within United States postal channels for foreign intelligence and counterintelligence purposes. It also applies to the opening of mail to or from U.S. persons where the mail is not in U.S. postal channels and the mail opening occurs outside the United States.

b. This chapter does not apply to searches of incoming and outgoing first-class mail at DOD incarceration facilities when authorized by their policy. Facility officials may provide pertinent information to Army CI as cooperating sources on the subjects of Army CI investigations who may be incarcerated at a DOD facility.

8–2. Mail searches within U.S. postal channels

a. United States postal regulations do not authorize MI to confiscate or open first class mail within United States postal channels, nor to request that the United States Postal Service (USPS) take such action on their behalf. However, MI may request appropriate law enforcement authorities to confiscate or open first-class mail within U.S. postal channels for law enforcement purposes under procedures established in DOD 4525.6–M, chapter 10.

b. MI may request that USPS authorities inspect or authorize the inspection of the contents of second-, third-, or fourth-class mail in United States postal channels, or request that USPS authorities confiscate mail that may become subject to search under this section.

8–3. Mail searches outside U.S. postal channels

a. MI is authorized to open first-class mail to or from a U.S. person outside USPS channels pursuant to Attorney General approval. Such requests are processed as nonconsensual physical searches under paragraphs 7–2*b* and 7–4.

b. MI is authorized to open mail outside USPS channels when both sender and recipient are not U.S. persons, if the search is otherwise lawful and consistent with applicable SOFAs.

c. The following officials may approve the searches in paragraph 8–3*b* within their areas of operation or areas under their jurisdiction. They may also delegate authority, in writing to their deputies, chiefs of staff, ranking intelligence officers, and subordinate corps, division, regional, installation, garrison, and MI brigade, group, and battalion commanders. No further delegation is authorized.

(1) DCS, G–2.
(2) Commander, U.S. Army Forces Central Command.
(3) Commander, Eighth U.S. Army.
(4) Commander, U.S. Army Europe.
(5) Commander, INSCOM.
(6) Commander, U.S. Army Pacific.
(7) Commander, U.S. Army South.
(8) Commander, U.S. Army Special Operations Command.
(9) Commander, 650th MI Group.

8–4. Mail cover

a. MI may request that USPS authorities examine mail (mail cover) in USPS channels, for counterintelligence purposes.

b. MI may request mail cover outside USPS channels in accordance with appropriate host nation law and procedures, and any SOFAs.

c. See paragraph 8–3*c* for approval authorities.

Chapter 9
Procedure 9: Physical Surveillance

9–1. General

This procedure applies to nonconsensual physical surveillance for foreign intelligence or counterintelligence purposes. It does not apply to physical surveillance conducted as part of a training exercise in which the surveillance subjects are

exercise participants. It also does not apply to countersurveillance, where MI personnel must detect foreign physical surveillance.

9–2. Physical surveillance of U.S. persons within the United States

a. MI may conduct nonconsensual physical surveillance of U.S. persons who are—

(1) Military personnel on active duty status.

(2) Present or former intelligence component employees.

(3) Present or former intelligence component contractors and their present or former employees.

(4) Applicants for intelligence component employment or contracting.

(5) Persons in contact with those who fall into categories 1 to 4, above, to the extent necessary to identify the person in contact.

b. Surveillance conducted outside a DOD installation under paragraph 9–2*a* must be coordinated with the FBI and other law enforcement agencies as appropriate.

c. Army CI may assist the FBI in conducting physical surveillance of U.S. persons, both on and off a DOD installation at FBI request, in accordance with the Delimitations Agreement and Army CI policy. When outside a DOD installation, Army CI may assist the FBI in those cases where a specific threat to DOD exists. Such surveillance may be approved by the Commander, INSCOM, who will keep the DCS, G–2 (DAMI–CDC) informed of activity taken under this section.

9–3. Physical surveillance of U.S. persons outside the United States

Outside the United States, MI may conduct nonconsensual physical surveillance of U.S. persons defined in paragraph 9–2*a*. MI may also place other U.S. persons under surveillance if—

a. The surveillance is consistent with host nation laws and policy and applicable SOFAs.

b. The surveillance is to collect significant foreign intelligence that cannot be obtained by other means.

c. The FBI, CIA, Naval Criminal Investigative Service (NCIS), or the Office of Special Investigations, U.S. Air Force (OSI) requests assistance.

9–4. Physical surveillance of non-U.S. persons

a. The officials identified in paragraph 9–5*a* may approve physical surveillance of non-U.S. persons for any lawful function assigned an MI element.

b. The authority to approve physical surveillance of non-U.S. persons outside the United States may be delegated down to no lower than an MI battalion commander, or equivalent. All delegations must be in writing.

c. Surveillance outside a DOD installation within the United States must be coordinated with the FBI and other law enforcement agencies, as appropriate.

9–5. Approvals

a. U.S. persons within DOD counterintelligence investigative jurisdiction. The officials below may approve physical surveillance of U.S. persons under DOD investigative jurisdiction, as stated in AR 381–20. The DCS, G–2 may delegate authority, as necessary. Other officials may delegate authority, in writing, through the chain of command to no lower than MI battalion commander, or his/her equivalent.

(1) DCS, G–2.

(2) Commander, U.S. Army Forces Central Command.

(3) Commander, Eighth U.S. Army.

(4) Commander, U.S. Army Europe.

(5) Commander, INSCOM.

(6) Commander, U.S. Army Pacific.

(7) Commander, U.S. Army South.

(8) Commander, U.S. Army Special Operations Command.

(9) Commander, 650th MI Group.

b. U.S. persons outside DOD investigative jurisdiction. Requests for physical surveillance of U.S. persons outside the United States who are not under DOD investigative jurisdiction will be forwarded to ODCS, G–2 (DAMI–CDC), for transmittal to the ATSD(IO). Confirmation of CIA coordination will be included. This coordination requirement does not apply to requests to assist the FBI, NCIS, and OSI, in which case the requesting agency would be responsible for obtaining appropriate approvals.

c. Surveillance for identification purposes. MI may conduct physical surveillance to identify persons in contact with a subject of a counterintelligence investigation, when approved by the officials in 9–5*a* or those to whom they have delegated authority. The MI element will notify the theater subcontrol office within 24 hours of the surveillance,

followed by written documentation to the subcontrol office and the Army Central Control Office within 48 hours of the surveillance. The written documentation will be transmitted electronically or via fax to meet the 48-hour requirement.

Chapter 10
Procedure 10: Undisclosed Participation in Organizations

10–1. General

This chapter will apply to MI personnel participating in any organization within the United States, or a U.S. person organization outside the United States, on behalf of MI. It will also apply when an employee is asked to take action within an organization for MI benefit, whether the employee is already a member or is asked to join an organization. Actions for MI benefit will include collecting information, identifying potential sources or contacts, and other activities directly relating to foreign intelligence or counterintelligence functions. It will not apply to—

a. Participation for purely personal reasons if undertaken at the MI employee's initiative and expense and for the employee's personal benefit.

b. MI personnel attending training programs for non-MI purposes (for example, leadership/management development and other training common to all Army organizations).

c. Cooperating sources who volunteer information obtained as a result of their participation in an organization. Information is volunteered when the source was not given prior direction or tasking to collect the information.

10–2. Criteria

Except as authorized below, MI personnel may participate in organizations on behalf of MI only if their MI affiliation is disclosed to an appropriate organization official, such as an organization executive officer or an official in charge of membership, attendance or organizational records. Undisclosed participation must—

a. Be essential to achieving a lawful foreign intelligence or counterintelligence purpose within the unit's assigned mission, and have prior approval of an official in paragraph 10–4.

b. Not be conducted within the United States to collect foreign intelligence from or about a U.S. person, or to collect information to assess a U.S. person as a potential source of assistance to foreign intelligence activities. This does not preclude collecting information volunteered by cooperating sources within the organization, if otherwise permitted by procedure 2.

c. Not include collection about the domestic activities of the organization or its members.

d. Last no longer than 12 months, unless an appropriate official re-approves participation. The approving authority will place the original signature approval document permanently in the file or dossier. Further dissemination is not required unless required by law or competent authority.

10–3. Participation types

a. General participation includes—

(1) Meetings open to the public, including professional seminars or conferences opened to members of a particular profession, whether or not they are members or received a special invitation.

(2) Organizations that permit U.S. Government employees to participate.

(3) Educational or professional organizations to enhance employee professional skills, knowledge or capabilities.

(4) Seminars, forums, conferences, exhibitions, trade fairs, workshops, symposiums, and similar meetings, when the employee is a member and was invited to participate, or when the sponsoring organization does not require disclosure of the participant's employment affiliation, so that the MI participant may collect significant foreign intelligence made available to general participants.

b. Specific participation includes meetings—

(1) To collect significant foreign intelligence outside the United States, or from or about non-U.S. persons within the United States.

(2) For counterintelligence purposes, at the FBI's written request.

(3) To collect significant counterintelligence about non-U.S. persons, or U.S. persons who are within DOD investigative jurisdiction. Participation within the United States requires FBI coordination.

(4) To identify and assess non-U.S. persons as potential foreign intelligence or counterintelligence sources.

(5) To collect information necessary to identify U.S. persons outside the United States as potential sources of assistance for foreign intelligence or counterintelligence.

(6) To develop or maintain an authorized cover.

(7) Outside the United States, to assess U.S. persons as potential sources of assistance to foreign intelligence or counterintelligence.

c. The following do not constitute undisclosed participation:

(1) Acquisition of goods and services that include incidental issuance of "membership" cards or identification (for example, video rental cards, library cards, grocery store cards, discount cards, gymnasium memberships).

(2) Any application, registration or subscription that does not result in actual attendance or participation in the activities of an organization covered under this procedure (for example, purchase of a subscription to an organization's magazine).

10–4. Approvals

a. The following officials, or their designees appointed in writing, may approve the participation listed in paragraph 10–3*a*:

(1) DCS, G–2.

(2) Commander, U.S. Army Forces Central Command.

(3) Commander, Eighth U.S. Army.

(4) Commander, U.S. Army Europe.

(5) Commander, INSCOM.

(6) Commander, U.S. Army Pacific.

(7) Commander, U.S. Army South.

(8) Commander, U.S. Army Special Operations Command.

(9) Commander, 650th MI Group.

b. The following officials or their single designees appointed in writing may approve the participation listed in paragraph 10–3*b*.

(1) DCS, G–2.

(2) Commander, INSCOM.

(3) Commander, U.S. Army Special Operations Command (authorized approval authority for para 10–3*b*(6) activities).

10–5. Disclosure requirement

a. When disclosure is required, the employee's intelligence affiliation will be provided to an executive officer of the organization or to an official in charge of membership, attendance, or the organization's records.

b. Disclosure may be made by the MI element, an authorized Army or DOD official, or another IC component authorized to make the disclosure on behalf of the MI element.

Chapter 11
Procedure 11: Contracting for Goods and Services

11–1. General

a. This chapter applies to MI personnel entering into contractual or similar arrangements with U.S. persons for the procurement of goods and services.

b. It does not apply to contracting with Government entities or MI personnel who enroll in academic institutions (governed by procedure 10).

c. No contract shall be void or voidable for failure to comply with procedure 11 guidance.

11–2. Contracts

a. Contracts with academic institutions. MI elements may contract with an academic institution after disclosing to appropriate institution officials the MI sponsorship.

b. Contracts with commercial organizations, private institutions and individuals. MI elements may contract with these elements without revealing MI sponsorship if one or more of the following applies:

(1) The contract is for published material available to the general public.

(2) The contract is for routine goods or services necessary for supporting approved activities, such as credit cards, car rentals, travel, lodging, meals, office or apartment rental, and other incidental items; and commercial on-line access services (Internet service provider).

(3) The Secretary of the Army or Under Secretary of the Army has signed a written determination that MI sponsorship must be concealed to protect an intelligence activity.

11–3. Additional considerations

MI elements and personnel will—

a. Not enter into contracts with U.S. Government employees without the approval of the head of the contracting activity.

b. Coordinate with the servicing legal advisor and the contracting office prior to acquiring intellectual property, patent, software, or data rights. MI employees will comply with all applicable law and policy, including AR 25–2 and Defense Federal Acquisition Regulation Supplement (DFARS), subpart 227.

c. Comply with the Joint Ethics Regulation, DOD 5500.7–R, and, when required, complete Office of Government Ethics (OGE) Form 450 (Executive Branch Confidential Financial Disclosure Report) and appropriate training.

d. Comply with fiscal law and policy. MI employees will not split purchases to avoid procurement or construction thresholds.

e. Comply with major acquisition rules requiring legal review under the provisions of DOD Instruction (DODI) 5000.2.

f. Ensure that secure environment contracts or acquisitions that are protected under the purview of special access programs allow access to appropriately cleared auditor personnel, legal counsel, inspectors general, and intelligence oversight personnel in accordance with DOD Directive (DODD) 5205.7.

g. Ensure that statements of work do not outsource inherently governmental activities as defined by Federal Acquisition Regulation (FAR) part 7.5 and Office of Federal Procurement policy.

h. Ensure that statements of work do not specify requirements for personal services. Ensure that contracts are not administered as personal services contracts (see FAR, part 36.104).

Chapter 12
Procedure 12: Assistance to Civilian Law Enforcement Authorities

12–1. General

a. This chapter specifies policy regarding MI assistance to U.S. civilian law enforcement authorities (CLEA) contained in EO 12333, as amended by EOs 13284 and 13355, DOD 5240.1–R, and the general limitations and approval requirements of DODD 5525.5.

b. Requests for support requiring approval under this procedure will be forwarded through command channels to the DCS, G–2 (DAMI–CDC) for further processing.

12–2. Cooperation with civilian law enforcement authorities

a. Upon approval of the Secretary of Defense, MI may assist CLEA for the following purposes:

(1) Investigating or preventing clandestine intelligence activities conducted by foreign powers, international narcotics organizations or international terrorist activities.

(2) Protecting DOD employees, information, property, facilities, and information systems.

(3) Preventing, detecting or investigating other violations of law.

b. Where MI is the lead agency of an investigation, MI may request assistance of CLEA as required.

12–3. Types of assistance

MI may assist civilian and military law enforcement with the following activities:

a. Disseminating incidentally acquired information reasonably believed to indicate a violation of Federal law. Disseminate in accordance with chapter 4 (procedure 4) (see also chap 16).

b. Disseminating incidentally acquired information reasonably believed to indicate a violation of state, local or foreign law. Disseminate in accordance with chapter 4 (procedure 4).

c. Providing specialized equipment and facilities to Federal authorities and, when lives are endangered, to state and local authorities, in accordance with DODD 5525.5.

d. Providing intelligence personnel to assist Federal authorities and, when lives are endangered, to state and local authorities, in accordance with DODD 5525.5 and with AGC concurrence.

e. Providing assistance to foreign government or foreign law enforcement and security services, in accordance with theater policy and applicable SOFAs.

12–4. Limitations

a. Intelligence personnel assigned or detailed to counter drug elements supporting CLEA must comply with the rules governing that agency and the rules under which the Army approved their assignment or detail.

b. Intelligence elements providing analytical support to CLEA will comply with DODD 5200.27 or the policy of the supported agency. The information under analysis is the property of the supported agency and is not intelligence information. Intelligence elements will provide the raw information and resultant analysis to the CLEA, and not retain the data in intelligence files or databases.

c. MI will neither request nor participate in the law enforcement or security activities conducted against U.S. persons by foreign governments or international organizations when the activities would not be authorized under this regulation.

d. DODD 5525.5 governs approval of nonintelligence specific training or expert advice (for example, training or advice common to many Army organizations, such as weapons familiarization, vehicle or communications equipment training, and so on). Commanders will provide an information copy to the ODCS, G–2 (DAMI–CDC) when approving such training by an intelligence component.

Chapter 13
Procedure 13: Experimentation on Human Subjects for Intelligence Purposes

13–1. General

a. This chapter applies to experimentation on human subjects whether or not they are a U.S. person, if conducted by or on behalf of an MI element. It does not apply to animal experimentation.

b. Experimentation is conducted on behalf of an MI element if—

(1) An MI element conducts the experiment.

(2) A contractor conducts the experiment on behalf of an MI element.

(3) A contractor conducts the experiment on behalf of a non-MI element for MI benefit.

(4) An MI element requests the experiment regardless of the existence of a contractual relationship.

13–2. Procedures

a. When required, a Human Use Committee must approve the experiment in accordance with AR 70–25.

b. The experiment must be conducted in accordance with Department of Health and Human Services guidelines, as implemented by AR 70–25.

c. The human subject must give informed, written consent.

d. Testing protocols must comply with AR 70–25.

13–3. Approvals

All proposals to conduct human subject testing will be forwarded to the ODCS, G–2 (DAMI–CDC), for Secretary of the Army, Under Secretary of the Army, Secretary of Defense, or Deputy Secretary of Defense approval as appropriate.

Chapter 14
Procedure 14: Employee Conduct

14–1. Training

a. All personnel conducting, supervising, or providing staff oversight of intelligence activities will be familiar with this regulation, with emphasis on chapters 1 through 4 and 14 through 17. Those who conduct, supervise, or provide staff oversight of the activities described in chapters 5 through 13 will be thoroughly familiar with the provisions of those procedures.

b. Commands will ensure personnel receive tailored unit training within 30 days of assignment or employment and refresher training as a part of the routine command training program.

c. To develop tailored training, units may download data from the intelligence oversight folders in the Army Knowledge Online or Army Knowledge Online-SIPRNET IC collaboration portals, or other appropriate web pages.

d. Commands that have signal intelligence cryptologic elements will ensure that those elements obtain appropriate training from qualified personnel on applicable Signal Intelligence directives.

14–2. Individual responsibilities

Individuals will—

a. Conduct intelligence activities in accordance with applicable law and policy, including EO 12333, as amended by EOs 13284 and 13355, DOD 5240.1–R, this regulation, and the policy of the appropriate intelligence discipline.

b. Familiarize themselves with this regulation and applicable Signal Intelligence directives as stated in paragraph 14–1.

c. Report questionable intelligence activities and Federal crimes upon discovery in accordance with chapters 15 and 16.

14–3. Command responsibilities

Commanders will ensure—

a. Personnel are protected from reprisal or retaliation because they report allegations in chapters 15 and 16. If

personnel are threatened with such an act, or if an act of reprisal occurs, they will report these circumstances to the DOD Inspector General.

b. Appropriate sanctions are imposed upon any employee who violates the provisions of this regulation or applicable USSIDs.

c. The field IG; the DCS, G–2; TIG; the AGC; the DOD General Counsel; and ATSD–IO (or the representatives of those officials) who have the appropriate security clearances are provided access to that information necessary to perform their oversight responsibilities, regardless of classification or compartmentation.

d. Employees cooperate fully with the President's Intelligence Oversight Board and its representatives.

e. All proposals for intelligence activities that may be unlawful, in whole or in part, or may be contrary to policy, will be referred to the AGC.

Chapter 15
Procedure 15: Questionable Intelligence Activities

15–1. General

a. This chapter provides a process for identifying, investigating, and resolving allegations of questionable intelligence activities. A reported allegation does not necessarily mean that a person or unit has violated law or policy. The fact that a questionable intelligence activity report has been submitted does not reflect negatively upon a unit; rather, it shows a unit's compliance with this regulation.

b. Only those questionable activities that are completed as part of MI duties or mission will be reported. Illegal or improper activities by MI personnel in their personal capacity that have no relationship to the intelligence mission (for example, breach of discipline, simple security or ethics violations) are not normally subject to intelligence oversight reporting and will be handled through normal disciplinary and law enforcement channels. Those personal actions that are reportable are listed in paragraph 15–4.

c. This chapter will not be used to satisfy other reporting requirements (for example, Serious Incident Reports (SIRs), Army CI incidents, or security violations).

d. Whenever in doubt as to whether an activity should be reported under this chapter, the activity will be reported as described herein for resolution at the higher level.

15–2. Reporting allegations

a. Employees and supervisors will report questionable intelligence activity upon discovery. Employees are encouraged to report questionable intelligence activity through command or inspector general channels to TIG (SAIG–IO), 1700 Army Pentagon, Washington, DC 20310–1700, with an information copy to the ODCS, G–2 (DAMI–CDC), 1000 Army Pentagon, Washington, DC 20310–1000. An employee may report directly to TIG (SAIG–IO), the DCS, G–2 (DAMI–CDC), the AGC, the ATSD–IO or the DOD General Counsel.

b. Regardless of which reporting channel used, the report must reach TIG (SAIG–IO) no later than five days from discovery. TIG will provide initial and final notifications of questionable intelligence activity to the ODCS, G–2 (DAMI–CDC) and the AGC.

c. Reports will describe the following:

(1) Identification of the personnel committing the alleged questionable intelligence activity by rank or civilian grade; security clearance and access; unit of assignment, employment, attachment or detail; and assigned duties at the time of the activity. Do not identify individuals by name or other personal identifier unless the TIG or DCS, G–2 (DAMI–CDC) so requests.

(2) When and where the activity occurred.

(3) A description of the activity and how it constitutes a questionable intelligence activity. The applicable portion(s) of this regulation and other applicable law or policy will be cited.

(4) Command and/or investigative agency actions planned or ongoing, if applicable. If this report originated outside the affected command, it will be stated when the reporting element notified the affected command. The TIG will then notify the affected command of their responsibility to conduct the inquiry and report updates.

d. Status reports will be submitted to TIG every 30 days until the investigation is completed. Once the investigation is completed, a final report will be submitted to TIG. The final report must be reviewed by the supporting judge advocate and will include corrective actions planned or implemented, command investigative status, personnel actions, and whether the unit has requested a policy clarification. When an allegation surfaces that is resolved within the five-day time frame specified in paragraph 15–2*b*, the report will be submitted as both an initial and a final report.

e. When an alleged questionable activity is the focus of a counterintelligence or criminal investigation, the investigating agency (INSCOM or the U.S. Army Criminal Investigation Command (USACIDC)) is responsible for submitting an initial notification of questionable activity to TIG. The investigating agency need not provide 30-day status reports under Procedure 15 to TIG on the progress of their investigation. This regulation does not relieve the

investigating agency of their normal investigative reporting procedures. When the investigating agency refers their investigative results to the affected command for action, the affected command must submit a final notification to TIG describing the investigative results and corrective actions taken, if any.

f. When there is doubt about whether an activity should be reported or someone in the chain of command disagrees with a questionable activity report from a subordinate unit, it will coordinate with the subordinate element to ensure the report meets reportable criteria as listed in paragraph 15–4. If the reportable criteria are not met, the report will be returned with instructions as to the proper reporting channel, if any. If the higher element is in doubt, or the two elements cannot agree, the report is forwarded to TIG (SAIG–IO) with an analysis of why the report does/does not meet reporting criteria. Before submitting the report, any command may contact the Office of TIG (SAIG–IO) or the ODCS, G–2 to seek clarification.

g. Reports may be transmitted via e-mail, facsimile, message, or hard copy, as long as they meet the 5-day requirement. An original signature hard copy is not required; electronic transmittal is preferred.

h. Reports may be classified at any level, including special access program caveats, as necessary for coherent reporting.

15–3. Inquiries

a. A command may choose to conduct an inquiry under the provisions of AR 15–6 or through an appropriate IG.

(1) Each report of questionable activity shall be investigated to the extent necessary to determine the facts and assess whether the activity is legal and is consistent with applicable policy.

(2) Inquiries into allegations not referred to a counterintelligence or criminal investigative agency will be completed within 60 days of the initial report, unless extraordinary circumstances dictate a longer period.

(3) The results will be reported in accordance with paragraph 15–2.

b. Such an inquiry does not alleviate or satisfy the initial 5-day reporting requirement in paragraph 15–2*b*.

15–4. Examples of questionable intelligence activity

The following are commonly reported questionable intelligence activities.

a. Improper collection, retention, or dissemination of U.S. person information. This includes—

(1) Gathering information about U.S. domestic groups not connected with a foreign power or international terrorism.

(2) Producing and disseminating intelligence threat assessments containing U.S. person information without a clear explanation of the intelligence purpose for which the information was collected (for example, listing area universities with foreign students or U.S. companies with DOD contracts in an assessment without showing a connection to a foreign power or international terrorism). An exception to this would be an MI element providing direct CI or technology protection support to a DOD contractor.

(3) Incorporating U.S. person criminal information into an intelligence product without determining if identifying the person is appropriate.

(4) Collecting U.S. person information for force protection purposes without determining if the intelligence function related to it is authorized (for example, collecting information on the domestic activities of U.S. persons).

(5) Submitting an CI incident report under AR 381–12 that contains information on a U.S. person suspected of committing a crime not related to national security, as opposed to passing the information directly to the responsible law enforcement or commander.

(6) Storing operations and command traffic about U.S. persons in intelligence files merely because the information was transmitted on a classified system.

(7) Collecting U.S. person information from open sources without a logical connection to the unit's mission or correlation to a validated collection requirement (for example, a unit in one area collecting information from the Web page of a militia group in another area, then reporting that information as a CI incident report or disseminating it in unit intelligence products).

(8) Disseminating command force protection information on U.S. person domestic activity as an intelligence product (for example, including U.S. person groups in an intelligence annex as enemy forces).

(9) Becoming directly involved in criminal investigative activities (for example, direct participation in a narcotics suspect interrogation) without prior AGC concurrence and Secretary of Defense approval.

(10) Identifying a U.S. person by name in an Intelligence Information Report without a requirement to do so.

(11) Including the identity of a U.S. person in a contact report when that person is not directly involved with the operation.

b. Misrepresentation. This includes—

(1) Using one's status as an MI member to gain access for non-MI purposes.

(2) Claiming to be conducting a highly classified activity or an investigation for personal gain, for unauthorized access, or to impress or intimidate another person.

(3) Using MI badge and credentials to represent oneself as an official beyond assigned MI responsibilities; to

perform functions not within the mission or authority of the element to which an individual is assigned or attached; or to avoid civil citations, such as off-duty traffic tickets.

c. Questionable intelligence activity constituting a crime. This includes—

(1) Stealing a source's payments.

(2) Using intelligence funds for personal gain.

(3) Falsifying intelligence or investigative reports.

(4) Stealing private property while searching for exploitable documents and materiel during a deployment.

(5) Stealing or allowing another to steal private property while using non-U.S. Government facilities for intelligence purposes.

(6) Searching or monitoring a U.S. person's private internet account, under the guise of determining if the individual was passing classified information, without an authorized counterintelligence or law enforcement investigation and proper search or electronic surveillance authority.

d. Misconduct in the performance of intelligence duties. This includes—

(1) Any activity listed in paragraphs 15–4*b* or *c*.

(2) Falsifying investigative reports or personnel security investigation interviews (also known as "curbstoning").

(3) Coaching a source or subject of an investigation prior to an intelligence polygraph examination in an effort to help the individual pass the polygraph.

15–5. Reports not meeting questionable intelligence activity criteria

Following are examples of reports that do not meet procedure 15 reporting criteria, unless there is a direct connection to an intelligence activity.

a. A report of someone acting without authority or exceeding authority that does not describe precisely the nature of the act and which chapter (1 through 13) or other Army policy was violated.

b. Security violations not directly connected to an intelligence activity, such as negligence in handling or storing classified information.

c. Not following regulations and other similar acts of personal misconduct appropriately dealt with through normal command actions, unless occurring during an intelligence activity or which meet Federal crimes reporting criteria.

d. Absence without leave or special category absentees.

e. Driving while intoxicated.

f. Drug use or sale.

g. Suicide or attempted suicide.

15–6. Inspectors general and general counsels

a. IGs, as part of their inspection of DOD intelligence components, and general counsels, as part of their oversight responsibilities, will seek to determine if such components are involved in any questionable activities. If such activities have been or are being undertaken, the matter shall be investigated in accordance with paragraph 15–3. If such activities have been undertaken but were not reported, the inspector general will also ascertain the reason for such failure and recommend appropriate corrective action.

b. IGs, as part of their oversight responsibilities, will, as appropriate, ascertain whether any organization, staffs, or office within their respective jurisdiction, but not otherwise specifically identified as DOD intelligence components, are being used for foreign intelligence or counterintelligence purposes to which Part 2 of EO 12333, as amended by EOs 13284 and 13355, applies. If so, the IGs will ensure that activities of such components are in compliance with this regulation and applicable DOD policy.

c. Each commander, supporting judge advocate, or IG will immediately report questionable activity of a serious nature to TIG, who will immediately notify ATSD(IO) and the DOD General Counsel, through the AGC.

d. TIG will submit a quarterly report to ATSD(IO) describing those activities that come to their attention during the quarter reasonably believed to be illegal or contrary to executive order or applicable DOD policy, and actions taken with respect to such activities. These reports will also include significant oversight activities undertaken during the quarter and any suggestion for improvement in the oversight system.

(1) TIG will coordinate the quarterly reports with the AGC prior to releasing the report to ATSD(IO). TIG will also provide a copy of the quarterly reports to ODCS–G2 (DAMI–CDC).

(2) To assist in preparing this report, the DCS, G–2; Commanding General, INSCOM; Commander in Chief, U.S. Army Europe; Commanding General, U.S. Army Forces, Central Command; and the Commanding General, Eighth U.S. Army will provide contributions not later than 15 days following the end of the quarter. These reports will be forwarded to TIG for inclusion in the quarterly report to ATSD(IO).

(3) Quarterly reports will include—

(a) A description of significant oversight activities undertaken during the quarter.

(b) Identification of unlawful or improper activities discovered or reported.

(c) Suggestions for improvement of the oversight system.

(4) Pursuant to AR 335–15, these quarterly reports are exempt from the requirement for a Requirements Control Symbol.

(5) All reports made pursuant to 15–6*c* and 15–6*d* that involve a possible violation of Federal criminal law will be reviewed by the general counsel concerned in accordance with the procedures adopted pursuant to EO 12333, section 1.7(a), as amended by EOs 13284 and 13355.

(6) The DOD General Counsel and the ATSD (IO) may review the findings of other general counsels and inspectors general with respect to questionable activities.

Chapter 16
Federal Crimes

16–1. General

This chapter implements DODI 5240.4 and the memorandum of understanding between the IC and Department of Justice prescribing IC procedures for reporting possible Federal crimes. The purpose is ensure that senior DOD and Department of Justice leadership is knowledgeable of serious Federal crimes involving MI employees and possible violations of Federal law by others that may come to the attention of intelligence personnel. This report does not replace existing investigative, judicial, or command authority and reporting requirements.

16–2. Reports

a. Reporting channel. Reports of Federal crimes involving MI personnel will be forwarded through command channels to the DCS, G–2 (DAMI–CDC), the PMG, and the USACIDC.

b. Time line. Reports will reach the ODCS, G–2 not later than 5 working days after discovery or receipt.

c. Contents. The following will be included in the report:

(1) Fullest possible identification of the person committing the alleged Federal crime: name, rank or civilian grade, social security number, military or civilian occupational specialty code, security clearance and present access, unit of assignment, employment, attachment or detail, and duties at the time of the activity.

(2) When and where the crime occurred.

(3) A description of the Federal crime that may have been violated.

(4) Identity of law enforcement agency receiving the report and investigating the incident.

(5) If the report originated outside the affected command, whether or not the command submitted its own report per this chapter or under the provisions of AR 190–40.

d. Reports flow. The DCS, G–2 will transmit reports received under this chapter to the AGC. The AGC will review and transmit reports received under this chapter pursuant to procedures adopted by the Department of Justice.

e. Unknown suspect. When the suspect's identity is unknown, as much detail as possible will be provided about the alleged crime. Clearly state that the suspect has not yet been identified and which agency is investigating. "John Doe" or other false names will not be used to refer to suspects. An additional report will be submitted when the suspect is identified.

f. "Bigot" cases. Normally, only the Army Central Control Office will report these cases. When the FBI already has an open investigation and is temporarily withholding the suspect's identity (known as a bigot case), the suspect will be identified as "John Doe 1, John Doe 2," and so on. In cases where the FBI has an open case and will report to the Department of Justice, an Army report will be rendered regarding the crimes listed in para 16–3, whether or not it is a bigot case.

g. SIRs. If a crime is reportable under the provisions of AR 190–40, an additional report under this chapter is not required. The AGC (SAGC) and the DCS, G–2 will be included as SIR addressees. Ensure that the report meets AR 190–40 time lines.

h. Additional reports. Federal crimes that are also questionable intelligence activities per procedure 15 will be reported, with an explanation of why the activity meets both criteria. If the unit initially reported per AR 190–40, the SIR date time group will be provided or a copy attached.

i. Current list. The HQDA Intelligence Oversight Web pages or the Army Knowledge Online or Army Knowledge Online–Siprnet IC collaboration portals will be sources for the most current list of reportable Federal crimes.

16–3. Reportable Federal crimes

Those crimes enumerated in paragraph 15–4*c* as well as the following are examples of crimes that meet the intent of this chapter:

a. Espionage.

b. Sabotage.

c. Unauthorized disclosure of classified information.

d. Seditious conspiracy to overthrow the U.S. Government.

e. Crimes involving foreign interference with the integrity of U.S. Government institutions or processes.

f. Crimes involving intentional infliction or threat of death or serious physical harm.

g. Unauthorized transfer of controlled technology to a foreign entity.

h. Tampering with, or unauthorized access to, information systems.

16–4. Nonreportable Federal crimes

The following are examples of crimes that do not meet the intent of this chapter:

a. Reportable information collected and disseminated to Army intelligence elements by another agency, unless MI was the sole recipient.

b. Crimes committed by nonintelligence employees who are under investigation by a criminal investigative organization.

c. Crimes against property totaling $500 or less for intelligence employees, or $1000 or less for other personnel.

d. Other than homicide or espionage, crimes that were committed more than 10 years before the Army intelligence element became aware of them. If, however, MI reasonably believes the criminal activities were or are part of a pattern of criminal activities, they are reportable no matter when the activity occurred.

Chapter 17
Support to Force Protection, Multinational Intelligence Activities, Joint Intelligence Activities, and Other Department of Defense Investigative Organizations

17–1. Command force protection programs

a. MI support to force protection may involve identifying, collecting, reporting, analyzing and disseminating intelligence regarding foreign threats to the Army, thereby enabling commanders to initiate force protection measures in accordance with AR 525–13.

b. In the United States, MI will limit such collection to foreign intelligence and international terrorism threat data, while efforts to collect, analyze, and disseminate U.S. criminal and domestic terrorism threat information will be restricted to Federal, State, and local law enforcement agencies.

c. Civilian Federal, State, and local law enforcement authorities have the primary responsibility for information collection to protect U.S. military forces within the United States.

d. USACIDC special agents serve as the Army's primary liaison representative to U.S. civilian law enforcement organizations and for exchanging criminal intelligence.

e. Army counterintelligence personnel serve as the Army's primary liaison representative to U.S. civilian law enforcement organizations for exchanging foreign threat information.

f. The PMG Antiterrorism Operations and Intelligence Cell, USACIDC, garrison provost marshals and security officers, and National Guard State Plans, Operations and Training Officers receive and disseminate time-sensitive threat information within the United States, regardless of source or type. As nonintelligence entities, they are not subject to the provisions of this regulation, but must comply with DODD 5200.27.

g. MI elements will not control force protection data bases within the United States in accordance with AR 525–13.

17–2. Multinational intelligence activities

a. Within multinational commands, if a foreign nation allows its personnel to conduct activities that U.S. personnel may not, a non-U.S. multinational intelligence unit commander may direct or authorize unit personnel to do so. However, U.S. personnel may not participate.

b. A U.S. Army commander of a multinational unit may not direct non-U.S. personnel to conduct activities that are lawful under other nations' laws, but prohibited by EO 12333, as amended by EOs 13284 and 13355.

c. If activities affecting U.S. persons, but not prohibited by EO 12333, as amended by EOs 13284 and 13355, were ongoing while another nation had command authority, the U.S. commander must gain U.S. component authority to continue the activity.

d. A U.S. judge advocate with intelligence law experience or training must review multinational intelligence activities for U.S. legal sufficiency.

17–3. Joint intelligence activities

Army personnel who are assigned to a joint command must be familiar with the policies of DOD and other military

intelligence organizations. Unless otherwise specified in writing by the joint force commander, the individual service component will comply with its service component intelligence policies.

17–4. Other Department of Defense investigative organizations

a. To the extent it does not conflict with Army CI functions, Army CI may cooperate with OSI and NCIS in performing Army CI functions.

b. Army CI may cooperate with OSI, NCIS, and USACIDC in automated intrusion investigations, criminal cases involving classified defense information, or other investigations in which these law enforcement elements have the lead, as specified in AR 381–20. Army CI need not have a concurrent open inquiry or investigation.

Appendix A
References

Section I
Required Publications

The following publications are available on the APD Web site (www.apd.army.mil) unless otherwise stated. DOD publications are available at www.dtic.mil/whs/directives. Public Law and U.S. Code are available at www.gpoaccess.gov/uscode.

AR 25–2
Information Assurance. (Cited in para 11–3*b*.)

AR 25–400–2
The Army Records Information Management System (ARIMS). (Cited in para 3–3*b*.)

AR 190–40
Serious Incident Report. (Cited in paras 1–4*f*, 16–2*c*(5), 16–2*f*, 16–2*g*.)

DODD 5525.5
DOD Cooperation with Civilian Law Enforcement Officials. (Cited in paras 12–1a, 12–2, 12–3*c*, 12–4*d*, 12–5*b*.)

50 USC 1805
Chapter 36, Foreign Intelligence Surveillance, Subchapter I, Electronic Surveillance: Issuance of Order. (Cited in para 5–1.)

Section II
Related Publications

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

AR 10–5
Organization and Function, Headquarters Department of the Army

AR 15–6
Procedures for Investigating Officers and Boards of Officers

AR 20–1
Inspector General Activities and Procedures.

AR 25–30
The Army Publishing Program

AR 70–25
Use of Volunteers as Subjects of Research.

AR 190–13
The Army Physical Security Program

AR 340–21
The Army Privacy Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–53
Information Systems Security Monitoring

AR 380–67
The Department of the Army Personnel Security Program

AR 381–12
Subversion and Espionage Directed Against the U.S. Army (SAEDA)

AR 381–20
The Army Counterintelligence Program

AR 525–13
Antiterrorism

DFARS
Subpart 227, Patents, Data, and Copyrights. (Available at www.acq.osd.mil/dpap/dars/dfars/index.htm.)

DOD 4525.6–M
Department of Defense Postal Manual

DOD 5240.1–R
Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons.

DOD 5500.7–R
The Joint Ethics Regulation (JER)

DODD 5200.27
Acquisition of Information Concerning Persons and Organizations Not Affiliated With the Department of Defense

DODD 5240.1
Department of Defense Intelligence Activities.

DODD 5205.7
Special Access Program (SAP) Policy

DODI 5000.2
Operation of the Defense Acquisition System

DODI 5240.4
Reporting of Counterintelligence and Criminal Violations.

EO 12333
United States Intelligence Activities. (Available at www.archives.gov/research/index.html.)

EO 13284
Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security. (Available at www.archives.gov/research/index.html.)

EO 13355
Strengthened Management of the Intelligence Community. (Available at www.archives.gov/research/index.html.)

FAR, Part 7.5
Inherently Governmental Functions. (Available at www.arnet.gov/far.)

FAR, Part 36.10401
Construction and Architect-Engineer Contracts: Policy. (Available at www.arnet.gov/far.)

P.L. 107–56
USA Patriot Act of 2001. (Available at www.archives.gov.)

5 USC 552
Freedom of Information Act

18 USC Chapter 119
Wire and electronic communications interception and interception of oral communications

18 USC 2511(2)(a)(i)
Interception and disclosure of wire, oral, or electronic communications prohibited

47 USC 605
Unauthorized publication or use of communications

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
The following forms are available on the APD Web site, www.apd.army.mil.

DA Form 11–2–R
Management Control Evaluation Certification Statement

OGE Form 450
Executive Branch Confidential Financial Disclosure Report

Appendix B
Management Control Evaluation Checklist

B–1. Function
The function of this checklist is to ensure effective implementation of the Army's intelligence oversight program.

B–2. Purpose
The purpose of this checklist is to assist commanders and intelligence oversight officials in evaluating the key management controls outlined below. It does not cover all controls, but focuses upon those that are essential for ensuring effective implementation of the intelligence oversight program.

B–3. Instructions
Answers must be based upon actual testing of key management controls such as document analysis, direct observation, interviewing, sampling, and simulation. Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These management controls *must* be evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2–R (Management Control Evaluation Certification Statement). All Army elements subject to the intelligence oversight program will develop and implement an intelligence oversight inspection program. This appendix may serve as a base for inspections, with additional questions as determined by the agency or command performing the inspection.

B–4. Test questions
a. Deputy Chief of Staff for Intelligence (DCS, G–2). Does the DCS, G–2—

(1) Promulgate policy, procedures, and programs necessary for implementing EO 12333, as amended by EOs 13285 and 13355, DODD 5240.1, and DOD 5240.1–R?

(2) Monitor, evaluate, and report on the administration of the intelligence oversight program?

(3) Ensure ACOM, ASCC, and DRUs and other agencies establish and maintain an ongoing self-inspection program, including periodic reviews and assessments of files and data bases containing U.S. person information?

b. Intelligence component commanders and staff as outlined in the applicability paragraph of this regulation. Has each commander—

(1) Established written local intelligence oversight policies and procedures?

(2) Initiated and supervised measures or instructions necessary to ensure U.S. person information is properly collected, retained and disseminated?

(3) Included intelligence oversight in the organizational inspection program?

(4) Ensured intelligence files are reviewed annually per paragraph 3–2?

c. Inspectors general.

(1) Has each IG identified all intelligence components subject to intelligence oversight inspection by the command?

(2) Is intelligence oversight included as part of the command's organizational inspection program?

(3) Are there procedures for determining if intelligence and supporting Staff Judge Advocate personnel of organizations understand and comply with the procedures in this regulation?

(4) Are procedures in place for determining if all intelligence personnel are trained in intelligence oversight upon initial assignment and periodically thereafter?

(5) Are procedures in place for determining if intelligence files are reviewed annually, per paragraph 3–2?

(6) Are questionable activities and Federal crimes committed by intelligence personnel reported as required?

(7) Are procedures in place to ensure that followup is conducted?

B–5. Comments

Help make this a better tool for evaluating management controls. Submit any comments to the DCS, G–2 (DAMI–CDC), 1000 Army Pentagon, Suite 2D350, Washington, DC 20310–1000.

Glossary

Section I
Abbreviations

ACOM
Army Command

AGC
Army General Counsel

AR
Army Regulation

ARIMS
Army Records Information Management System

ARNG
Army National Guard

ASCC
Army Service Component Command

ATSD–IO
Assistant to the Secretary of Defense for Intelligence Oversight

CI
Counterintelligence

CIA
Central Intelligence Agency

CIO/G–6
Chief Information Officer/G–6

CLEA
civilian law enforcement agency

DA
Department of the Army

DCS, G–2
Deputy Chief of Staff, G–2

DCS, G–3/5/7
Deputy Chief of Staff, G–3/5/7

DFARS
Defense Federal Acquisition Regulation Supplement

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DRU
Direct Reporting Unit

EO
Executive Order

FAR
Federal Acquisition Regulation

FBI
Federal Bureau of Investigation

FISA
Foreign Intelligence Surveillance Act

FISC
Foreign Intelligence Surveillance Court

FN
File number

IC
Intelligence community

IG
Inspector general

INSCOM
Intelligence and Security Command

IP
Internet protocol

MI
Military intelligence

NCIS
Naval Criminal Investigative Service

NGB
National Guard Bureau

ODCS, G–2
Office of the Deputy Chief of Staff, G–2

OGE
Office of Government Ethics

OSI
Office of Special Investigations, U.S. Air Force

PMG
Provost Marshal General

SIR
Serious Incident Report

SOFA
Status of Forces Agreement

TIG
The Inspector General, Army

TRADOC
U.S. Army Training and Doctrine Command

TSCM
Technical Surveillance Countermeasures

URL
Uniform Resource Locator(s)

USACIDC
U.S. Army Criminal Investigation Command

USC
United States Code

USPS
United States Postal Service

Section II
Terms
Some terms differ substantially from traditional IC or Army usage.

Administrative purposes
Information is collected for "administrative purposes" when it is necessary to administer the intelligence component, but is not collected directly in performance of an intelligence activity. Examples include general correspondence files; employment and disciplinary files; training records; in and out processing files; systems administration backup records; contractor performance records; personnel security clearance and access records; security manager duties; public affairs and legislative support materials. Administrative purposes may also include individual hand receipts and other logistics records staff actions, executive summaries and other information papers/briefings provided to senior leadership, and activity financial documents.

Collection
Information is collected when it is gathered or received by an intelligence employee in the course of official duties, and is intended for intelligence use. An employee must take an action that demonstrates an intent to use or retain the information, such as producing an intelligence information or incident report or adding the information to an intelligence database. Data acquired by electronic means (for example, telemetry, signals traffic analysis, measurement and signatures intelligence) is "collected" only when it has been processed from digital electrons into a form intelligible to a human. Information that is held or forwarded to a supervisory authority solely for a collectability determination, and not otherwise disseminated within the intelligence component, is not "collected."

Computer trespasser
One who accesses a protected computer without authorization, and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer (see 18 USC 2510 (21)(a)).

Concealed monitoring
Targeting a particular person or group without their consent, in a surreptitious and continuous manner, by electronic, optical, or mechanical devices. Monitoring is surreptitious when it is conducted in a manner designed to keep the subject unaware of it and continuous if conducted without interruption for a substantial time.

Consensual intercept
Electronic surveillance conducted after one or more, but fewer than all, of the parties to a communication consent to the interception.

Consent
An oral or written agreement by a person or organization to permit MI to take particular actions that affect the person or organization. Consent is implied upon adequate notice that a particular action carries the presumption of consent to an accompanying action (for example, notice that entering a building constitutes consent to being searched).

Cooperating sources
Persons or organizations that knowingly and voluntarily provide information, or access to information, to MI, either upon request or on their own initiative. These include Government agencies, law enforcement authorities, credit

agencies, academic institutions, employers, and foreign government representatives and organizations. Cooperating sources must know that they are dealing with an intelligence component.

Counterintelligence
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.

Delimitations Agreement
Common term for the DOD/Department of Justice Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation.

Domestic activities
Activities within the United States that do not involve a significant connection with a foreign power, organization, or person.

Electronic surveillance
Electronic surveillance is composed of the following:

a. The acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known U.S. person who is in the United States, if the contents are acquired by intentionally targeting that U.S. person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

b. The acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, but does not include the acquisition of those communication of computer trespassers that would be permissible under section 18 USC 2511(2)(i).

c. The intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States.

d. The installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes (see 50 USC 1801).

Electronic surveillance outside the United States
Acquisition of a nonpublic communication by electronic means without the consent of a party to the communication or, in the case of a non-electronic communication, without the consent of a person who is visibly present at the place of communication. This does not include the use of radio direction finding equipment solely to determine the location of a transmitter. Electronic surveillance is outside the United States if the target is physically outside the United States, regardless of the location from which the surveillance is conducted.

Employee
A person assigned to, employed by, detailed to, or acting for an MI element, including contractors and other persons acting at MI direction. Also referred to as MI personnel in the plural.

Experimentation
Any research or testing activity involving human subjects that may expose them to the possibility of permanent or temporary injury, whether physical or psychological damage, or damage to reputation, beyond the ordinary risks in their daily lives.

Force protection
A commander's program to protect personnel, family members, facilities, and material, in all locations and situations. It is accomplished through the planned and integrated application of operations security, combating terrorism, physical security, base defense, personal protective services, law enforcement and crime prevention. The program is supported by intelligence, counterintelligence, and other security programs (see AR 525–13).

Foreign intelligence
Information about the activities, capabilities, plans and intentions of foreign powers, organizations, and persons, and their agents, but not including counterintelligence except for information on international terrorist activities.

Foreign power
Any foreign government, whether or not recognized by the United States, foreign-based political party or faction thereof, foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities.

Hearability survey
Monitoring radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the reception quality over time.

Incidental acquisition
Information about a nontargeted U.S. person received during an authorized intelligence activity.

Intelligence activities
Activities necessary for the conduct of foreign relations and the protection of the national security, including—

a. Collecting information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities.

b. Intelligence dissemination and production.

c. Collecting information concerning, and conducting activities to protect against, intelligence activities directed against the United States, international terrorist and international narcotics activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents.

d. Special activities.

e. Administrative and support activities within the United States and abroad necessary for performing authorized activities.

f. Such other intelligence activities as the President may direct from time to time (see EO 12333, as amended by Eos 13284 and 13355).

Intelligence community (IC)
The Director of Central Intelligence staff; Central Intelligence Agency; Defense Intelligence Agency; National Imagery and Geospatial Agency; National Reconnaissance Office; National Security Agency; the Department of State Bureau of Intelligence and Research; and the intelligence elements of the Army, Navy, Air Force, Marine Corps, Coast Guard, Federal Bureau of Investigation, Department of Energy and Department of the Treasury.

Intelligence oversight staff officer
An individual with a background in military intelligence who assists the commander in carrying out his intelligence oversight responsibilities (for example, ensuring the propriety of all planned and on-going intelligence activities; identifying, investigating, and reporting questionable intelligence activities).

International narcotics activities
Activities outside the United States to produce, transfer or sell narcotics or other substances controlled in accordance with 21 USC 811–812.

International terrorist activities
Activities undertaken by or in support of terrorist or terrorist organizations that occur totally outside the United States, or that transcend national boundaries in the manner by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

Mail cover
Making a record of any data appearing on the outside cover of any class of mail as permitted by law, other than that necessary for mail delivery or postal service administration. Also referred to as examination of mail.

Mail within United States postal channels
Such mail includes—

a. Mail while in transit within, among, and between the United States, its territories and possessions.

b. Foreign originated mail passed to United States postal channels, or transiting the United States mail system to another foreign mail service under a postal treaty or convention.

c. Mail temporarily in the hands of the Customs Service, Department of Agriculture, Army-Air Force and Navy post offices.

d. Mail for delivery to the United Nations.

e. Mail is considered in United States postal channels until the moment it is manually delivered to the specific

addressee named on the address label, or his authorized agent. U.S. postal channels do not include private corporations that provide correspondence and package shipping services outside USPS channels.

Multinational intelligence activities
Intelligence activities conducted by deployed multinational units or task forces, such as a NATO Allied Military Intelligence Battalion.

Organization
Corporations and other commercial entities, academic institutions, clubs, professional societies, associations, and other groups whose existence is formalized in some manner or otherwise function on a continuing basis.

Organization within the United States
All organizations physically located within the United States' geographical boundaries, whether or not the organization is a U.S. person.

Overt means
Methods of collection whereby the information source is told, or is otherwise aware, that he is providing information to DOD or a DOD component.

Participation in an organization
Any action undertaken within an organization's structure or framework. Includes serving as an organization agent or representative; becoming a member; attending meetings not open to the public, including organizational social functions; carrying out the work or functions of the organization; and contributing funds other than in payment for goods and services.

Pen register
A device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business (see18 USC 3127(3) and trap and trace).

Permanent resident alien
A foreign national lawfully admitted into the U.S. for permanent residence (a "green card" holder).

Physical search
Physical search includes—

a. Any intrusion upon a person or a person's property or possessions to obtain property or information. It does not include areas that are in plain view and visible to the unaided eye if no physical trespass occurs, abandoned property left in a public place, or any intrusion authorized as necessary to accomplish lawful electronic surveillance.

b. Any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes (see50 USC 1821(5)).

Physical surveillance
Systematic and deliberate observation of a person by any means on a continuing basis. Acquiring a nonpublic communication by a person not party to it or not visibly present, through any means not involving electronic surveillance (that is, not intercepting and/or recording the communication).

Publicly available
The information has been published or broadcast in media available to anyone who wishes to obtain it. Examples include unrestricted web pages, books, newspapers, magazines, professional journals, radio, public address systems and television.

Questionable intelligence activity
Conduct during or related to an intelligence activity that may violate law, Executive Order or Presidential Directive, or applicable DOD or Army policy, including this regulation.

Reasonable belief
The facts and circumstances are such that a trained and experienced reasonable person would hold the belief. Reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. It can be based upon experience, training, and knowledge in foreign intelligence or counterintelligence work applies to facts and circumstances at hand so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not. Also referred to as probable cause.

Retention
Refers only to maintaining information about U.S. persons that can be retrieved by the person's name or other personal identifying data.

Special activities
Activities conducted in support of national foreign policy objectives abroad, planned and executed so that the role of the U.S. Government is not apparent or publicly acknowledged. These activities are not intended to influence United States political processes, public opinion, or media, and do not include diplomatic activities or the collection and production of intelligence.

Trap and trace device
A device which captures the incoming electronic or other impulses which identify the origination number of an instrument or device from which a wire or electronic communication was transmitted (see 18 USC 3127(4) and pen register).

United States
All areas under the territorial sovereignty of the United States, that is, States, districts, commonwealths, territories, possessions, and jurisdictional waters.

United States person
A U.S. citizen; an alien known by the intelligence component to be a permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; a corporation incorporated in the United States that is not directed or controlled by a foreign government. A corporation or a subsidiary incorporated abroad is not a U.S. person even if partially or wholly owned by a corporation incorporated in the United States.

Vulnerability survey
Acquiring radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to foreign intelligence interception.

Section III
Special Abbreviations and Terms
This section contains no entries.