

9 January 2010

Military Intelligence

EIGHTH UNITED STATES ARMY ESPIONAGE PREVENTION AND SUBVERSION AND
ESPIONAGE DIRECTED AGAINST THE ARMY PRIMER

***This regulation supersedes Eighth Army Pamphlet 381-12, 8 June 1990.**

FOR THE COMMANDER:

LEWIS F. SETLIFF III
Colonel, GS
Chief of Staff

OFFICIAL:



GARRIE BARNES
Chief, Publications and
Records Management

Summary. This pamphlet clarifies reporting requirements and organizations in reference to Army Regulation (AR) 381-12 to assist all Eighth United States Army (EUSA) personnel to better identify indicators of espionage, terrorism, sabotage, subversion, theft or diversion of military technology, information systems intrusions, and unauthorized disclosure of classified information and gives information on how to report such incidents.

Applicability. This pamphlet applies to United States (US) soldiers and civilian employees (including US contractors) and their family members and local national employees.

Supplementation. Supplementation of this regulation and issuance of command and local forms is prohibited unless prior approval is obtained from HQ, 8th Army, G2, APO AP 96205-5260.

Forms. AK Forms are available at http://8tharmy.korea.army.mil/g1_ag/.

Records management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System website at <https://www.arims.army.mil>.

Suggested improvements. The proponent of this pamphlet is the Office of the Assistant Chief of Staff, G2. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, EUSA, ATTN: G2, APO AP 96205-0260.

Distribution. Electronic Media Only (EMO).

[Counterintelligence Points of Contact](#)

COUNTERINTELLIGENCE POINTS OF CONTACT

Theater –wide 24 Hour Hot Line: SAEDA-99 (DSN 723 – 3299)

Commercial: 0505 723-3299

Uijongbu Office: (DSN) 732-7058 / 6761 – Available during normal duty hours

After duty hours: Cell 011-695-0370

Seoul Office: (DSN) 736-6387 / 3299 - Available during normal duty hours

After duty hours: Cell 011-9252-9236

Pyongteak/Wonju/USAG-Humphreys Office: (DSN) 753-8157 / 8155 – Available during normal duty hours

After duty hours: Cell 010-3100-0171

Waegwan Office: (DSN) 765-7327 / 7359 - Available during normal duty hours

After duty hours: Cell 011-9252-1439

Daegu Office: (DSN) 768-6768 / 6776 – Available during normal duty hours

After duty hours: Cell 011-695-0763

Busan Office: (DSN) 763-3314 / 3366 - Available during normal duty hours

After duty hours: Cell 011-9909-0993

Kwangju Office: (DSN) 786-6027 / 6626 - Available during normal duty hours

After duty hours: Cell 011-9909-0027

For more information, contact 524 MI Bn Current Operations (CUROPS) at DSN: 723-9953 / 7719 or email 501MI-524S2X@mi.army.mil. Additionally, you can contact EUSA G2X, at 723-6600 / 7239.

CONTENTS

Chapter 1

Introduction, pages 4

- 1-1. Purpose
- 1-2. References
- 1-3. Explanation Of Abbreviation and Terms
- 1-4. Responsibilities

Chapter 2

Reporting Requirements, pages 6

- 2-1. Reportable CI Incidents and Situations
- 2-2. Additional Matters of CI Interest

Chapter 3

Reporting Procedures, pages 11

- 3-1. Individual Response
- 3-2. Report The Incident To The Authorities
- 3-3. Contacted Personnel
- 3-4. False Reporting

Chapter 4

CI Awareness and Education, pages 12

- 4-1. The Army as a Target
- 4-2. Importance of DA Employee Participation
- 4-3. Policy
- 4-4. Training Conduct
- 4-5. Training Content
- 4-6. Vulnerable Personnel and Positions
- 4-7. Conduct of Special Category Briefings (SCB) and Debriefings.

Appendixes A. References, pages 17

Table 2-1. Espionage Indicators, pages 9

Glossary, pages 20

Chapter 1

Introduction

1-1. Purpose

The main objective of this regulation is to assist all members of EUSA in detecting foreign intelligence collection and international terrorist threats against the Army. This is accomplished through an awareness program designed to ensure that all EUSA members recognize and report incidents and indicators of attempt to actual espionage, subversion, sabotage, terrorism directed against the US Army and its personnel, facilities, resources and activities; illegal diversion of military technology; unauthorized intrusions into automated information systems; unauthorized disclosure of classified information; and other reportable CI incidents.

1-2. References

Required and related publications and prescribed and references forms are listed in Appendix A.

1-3. Explanation of Abbreviation and Terms

Abbreviations and special terms used in this pamphlet are explained in glossary.

1-4. Responsibilities

a. Individual Responsibilities. All EUSA employees (See Glossary) will –

- (1) Be knowledgeable of matters which should be reported to CI authorities.
- (2) Be knowledgeable on which CI unit to report an incident.
- (3) Report incidents listed in Chapter 2.
- (4) Follow reporting procedures listed in Chapter 3.
- (5) Cooperate with CI Agents for the conduct of Special Category Briefings (paragraph 4-6) and debriefings when requested.
- (6) Cooperate and render assistance to all CI Agents in the conduct of their official duties.
- (7) Not discuss or disclose information provided to or discussed with a CI Agent outside of investigative channels.

b. All EUSA Unit Commanders. Army Commanders at all levels will –

- (1) Report all CI incidents or matters identified in Chapter 2 to an Army CI element within 24 hours after an incident is discovered (paragraph 3-2).
- (2) Place command emphasis on the importance of CI reporting and the penalties for not reporting.
- (3) Incorporate CI training into unit training schedules, and ensure all assigned and employed personnel receive annual CI training, including Army contractors in accordance with contractual requirements.
- (4) Identify those personnel who should receive CI special category briefings and ensure they are briefed by CI Agents.

(5) Ensure that knowledge of CI incidents is limited by reporting incidents directly to supporting CI offices whenever possible. This restricting preserves the integrity of any ensuing investigation.

(6) Monitor the CI awareness program to ensure that –

(a) Their unit coordinates with the supporting CI office or organic CI personnel to provide input and better tailor the desired CI training.

(b) Training included those topics required by Chapter 4.

(c) All CI Awareness and Reporting training will be conducted by certified CI trainers (paragraph 1-4c and 4-4b).

(d) Continuous CI program publicity is developed and implemented.

(e) All personnel cooperate with CI Agents in the debriefings specified in paragraph 4-2.

(7) Include CI Awareness and Reporting as part of the unit command inspection program.

(8) Prior to a deployment, identify the supporting CI unit and then determine theater-approved policy and procedures to securely and quickly report a CI incident.

(9) Coordinate with security managers and S2 officers to ensure that they are aware of those matters which are of potential CI interest and that they know how to contact the supporting CI office to refer such reports.

(10) Maintain name, date and section records of personnel trained per local standard operating procedures and unit administrative policies.

c. EUSA Unit commanders with CI personnel assigned / attached. 2ID and 501 MI BDE will --

(1) Ensure that a CI Awareness and Reporting program is a key functional area that supports all Army commanders in the unit's mission and area of responsibility.

(2) Establish standards for all CI Awareness and Reporting trainers and certify that the CI unit trainers (see paragraph 4-4b) can conduct CI Awareness and Reporting training and meet Army and unit standards.

(3) Ensure CI education and briefings are tailored to the mission, location, and degree of potential foreign threat to supported units. Units with organic CI Special Agents may develop and present CI training internally, but will coordinate with the supporting CI office to acquire material which is recent and relevant.

(4) Coordinate with supported commands to identify those personnel who require Special Category Briefings, and ensure tailored briefings are prepared and conducted.

(5) When authorized, debrief personnel as specified in paragraphs 4-6 and 4-7.

(6) Ensure that Army personnel reporting CI incidents are interviewed as soon as possible and submit the CI incident report (CIR) within 72 hours of the incident being reported to a CI unit directly to the G2X with information copies to the EUSA CDR.

(7) Include the CI awareness and reporting program and support to Army customers as part of the unit command inspection program.

(8) Produce an internal memorandum for record for each CI Awareness Briefing.

* Record:

- Briefer's name.
- Briefing purpose (annual requirement, deployment, special activity, etc.).
- Briefing time, date, and location.
- Supported unit/organization.
- Number of attendees.
- Comments(e.g. scheduled follow-on debriefings, scheduled one-on-one briefings, received a CI Incident Report, referred lead to another organization, request for information by supported unit, produced other threat or intelligence reports).

(9) Produce a quarterly memorandum for record to assess the effectiveness of the CI unit's CI Awareness Program per paragraph 6-2 of AR381-12.

Chapter 2 Reporting Requirements

2-1. Reportable CI Incidents and Situations

All EUSA employees must report the incidents described in this paragraph; failure to comply will result in judicial or administrative action. All EUSA employees must be familiar with these situations and related indicators of espionage (see table 2-1). A single indicator **does not** necessarily mean that a person is engaged in espionage. Reporting the situation to the supporting CI office will allow the authorities to better assess the situation. Reporting procedures are listed in Chapter 3 of this pamphlet. Report:

a. Attempts by unauthorized persons to obtain classified or controlled unclassified information concerning DoD facilities, activities, personnel, technology, or material through questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence (includes electronic correspondence), or automated systems intrusions.

b. Acts of or plans to commit treason, spying or espionage.

c. Contact with people known or suspected to be members of, or associated with, foreign intelligence, security, or international terrorist organizations. This does not include contracts which DA employees have as part of their official duties, unless that foreign official or citizen—

(1) Exhibits excessive knowledge or undue interest about the DA member or his duties which is beyond the normal scope of friendly conversation.

(2) Exhibits undue interest in U.S. technology, research, development, testing, and evaluation efforts; weapons and intelligence systems; or scientific information.

(3) Attempts to obtain classified or controlled unclassified information.

(4) Attempts to place DA employees under obligation through special treatment, favors, gifts, money, or other means.

(5) Attempts to establish business relationships that are outside the range of normal official duties.

(6) Suddenly stops asking about specific technology, research, development, testing, and evaluation efforts; weapons and intelligence systems; or scientific information, when the foreign national had been previously interested (see anomaly in glossary).

d. Incidents in which EUSA employees or their family members traveling to or through foreign countries or in CONUS are contacted by possible foreign law enforcement, security, or intelligence officials and---

(a) Questioned about their duties.

(b) Requested to provide classified or controlled unclassified information.

(c) Threatened, coerced, or pressured in any way to cooperate with a foreign intelligence service or foreign official.

(d) Offered assistance in gaining access to people or locations not routinely afforded Americans.

e. Contact with a foreign diplomatic establishment, whether in the U.S. or abroad, for personal or official reasons. Personnel in sensitive positions will apprise their security managers in advance of the nature and reason for contacting a foreign diplomatic establishment.

f. Known, suspected, or possible unauthorized disclosure of classified or controlled unclassified information, including leaks to the media.

g. Unauthorized and unreported removal and retention of classified document or material.

h. Information concerning any international terrorist activity or foreign directed sabotage that poses an actual or potential threat to Army or other U.S. facilities, activities, personnel, or resources.

i. Active attempts to encourage EUSA personnel to violate laws, disobey lawful orders or regulations, or disrupt military activities (subversion).

j. EUSA personnel participating in activities advocating or teaching the overthrow of the United States government by force of violence, or seeking to alter the form of government by unconstitutional means (sedition).

k. Known or suspected intrusions by a foreign entity into classified or unclassified automated information system by unauthorized users or by authorized users attempting to gain unauthorized access; and unauthorized transmissions of classified or unclassified controlled information over commercial communications means, whether originated from work or elsewhere.

l. Attempted or actual coercion, influence, or pressure brought to bear on EUSA personnel through family members.

m. Discovery of a suspected listening device or other technical surveillance device. Do not disturb the device or discuss the discovery in the affected area. Immediately report its presence in-person or via secure communications, away from/outside of the site/facility of suspicion, avoiding the area which the suspected device is located.

n. U.S. military personnel who defect to another nation, attempt or threaten to defect, and the return to military control of U.S. military defectors.

o. Suspected volunteer spy, or an insider threat.

p. Online socialization (e-mail, blog, chat room, dating) with a person who attempts to obtain classified or unclassified military information, exhibits excessive knowledge or interest about the Army member or his duties, or attempts to place Army personnel under obligation.

q. Any incidents where U.S. Government owned laptop computers or other portable computing and data storage devices are known or suspected of having been tampered with while on official travel in a foreign country. Such tampering often occurs when the device is left unattended in a hotel room. If tampering is suspected, refrain from turning it on or using the device and provide it to the servicing CI office immediately upon return.

2-2. Additional Matters of CI Interest

The following are additional matters which should be reported expeditiously to the nearest CI office:

a. Special Category Absentees. Unauthorized or unexplained absence of EUSA personnel who, within the year preceding the absence, have had access to SECRET, TOP SECRET, or cryptographic information, special access program information or sensitive compartmented information, or an assignment to a special mission unit. This report is in addition and secondary to the immediate report to the Provost Marshal required by AR 630-10.

b. Suicide involving EUSA employees with access to classified information. A EUSA employee's attempted to actual suicide, when the member had an intelligence background, was assigned to a special mission unit, or within the last year had access to classified material.

c. Detention of EUSA personnel and/or family members by a foreign power.

d. Impersonation of Military Intelligence Personnel, or the unlawful possession or use of US Army Intelligence identification, such as badges and credentials. This report allows MI to assess damage, while criminal investigative organizations investigate the crime.

e. Compromise of US Intelligence Personnel Identities. Willfully compromising the identity of US intelligence personnel engaged in foreign intelligence and counterintelligence activities. This report allows MI to assess damage, while criminal investigative organizations investigate the crime.

f. Weapons of Mass Destruction, Critical Technology. Incidents in which foreign countries offer employment to US personnel in the design, manufacture, maintenance, or employment of weapons of mass destruction, or other critical technology fields. This report allows military intelligence to track which technologies are targeted for foreign collection.

**Table 2-1
Espionage Indicators**

Behavior	Indicator(s)
Contact with foreigners	<ul style="list-style-type: none"> • Unauthorized contact with an individual who is known or suspected of being associated with a foreign intelligence, security, or terrorist organization. • Frequent or regular contact with persons with interest contrary to those of the US. • Frequently and without explanation taking short foreign trips. • Either in CONUS or OCONUS, visits to a foreign embassy, consulate, trade, or press office, or other unreported contact with foreign officials, outside the scope of one's official duties.
Disregard for security practices	<ul style="list-style-type: none"> • Removing classified computer storage media and other materials from work area or unauthorized possession of classified materials outside work areas. • Reading or discussing classified or controlled unclassified information in unauthorized locations. • Improperly removing security classification markings from documents and computer media. • Requesting witness signatures on classified document destruction forms when the proposed witness did not actually observe the destruction. • Bringing unauthorized cameras, recording or transmission devices, computers, modems, electronic storage media, or software into areas where classified data is stored, discussed, or processed. • Repeated involvement in security violations. • Repeated involvement in the movement of classified data from DoD computer systems, outside of authorized Electronic Media Transfer Authority Channels.
Unusual work behavior	<ul style="list-style-type: none"> • Attempts to expand classified information access by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities, or attempts to obtain information for which the person has no authorized access or need to know. • Extensively using copy, facsimile, document scanners, or other automation equipment to reproduce or transmit classified material, exceeding actual job requirements. • Attempts to escalate computer account privileges or access, by social engineering or through circumventing information security mechanisms, to obtain information for which the person has no legitimate access or need to know. • Repeatedly performing unaccompanied classified work outside of normal duty hours, especially unaccompanied. • "Homesteading" (repeatedly requesting tour of duty extensions in one assignment or location), which the assignment offers significant access to classified information. • Offering extra income from an outside endeavor to personnel with sensitive jobs or access, or attempting to entice them into criminal situations, which could lead to blackmail or extortion.

Behavior	Indicator(s)
Undue affluence	<ul style="list-style-type: none"> • Unexplained or undue affluence without a logical income source, e.g., free spending, lavish display of wealth, a bad financial situation suddenly reverses, opening several bank accounts containing substantial sums of money, or sudden large debt or loan repayment. • Attempts to explain wealth as inheritance, gambling luck, or successful business venture, without apparent verification
Unexplained foreign travel	<ul style="list-style-type: none"> • Frequently and without explanation taking short foreign trips or travel in the United States to cities with a foreign diplomatic presence. • Travel appears unusual or inconsistent with a person's interest or financial means. <p>NOTE: Civilian employees with access to SCI are required to report foreign travel to their security managers prior to departure.</p>
Undue interest	<ul style="list-style-type: none"> • Uncomfortable persistent questioning of your duties, missions, functions, access to information (classified and unclassified), technology, research, development, testing, etc. • Uncomfortable attempt to befriend or recruit you for the purposes of obtaining DA information (written, electronic, or verbal), classified or unclassified. • Any attempt by an unauthorized person to gain access to Army information (classified, controlled unclassified). • Any attempt to gain Army information without having a need to know.
Ego	<ul style="list-style-type: none"> • Joking or bragging about working for a foreign intelligence service.
Internet activities	<ul style="list-style-type: none"> • Unjustifiable and frequent browsing of internet websites promoting or advocating known terrorist organizations and groups, extremist themes, the construction of explosives and weapons, or other terrorist related activities. • Browsing of Internet websites owned by diplomatic establishments and other official websites of adversarial governments in an apparent attempt to obtain email addresses or directions to a foreign diplomatic facility. • Actively participant in the Internet "chat" websites, message boards, or "Blogs" which promote or advocate terrorism and extremist themes. • Manipulating, exploiting or "hacking" computer systems or local networks in attempt to gain unauthorized access.

g. Research and Technology Protection. Known or suspected compromise, collection or diversion of US technology or weapon systems by anyone for the benefit of a foreign government. This includes attempts to compromise, collect or diver US technology and threats to trusted insiders.

h. Suspected of known anomalies (see Glossary, Section II, terms).

Chapter 3 Reporting Procedures

3-1. Individual Response

Persons who knows or involved in a CI reportable incident should:

- a. Remain calm.
- b. Neither refuse, nor agree to cooperate with an approach, but don't commit.
- c. DO NOT conduct your own investigation or attempt to follow the other persons involved.
- d. Recall the incident date, time, and place; physical description and identity, if known; license number and description of any vehicle involved, if known; witness identities and other who know about it; and details of the incident.
- e. Limit knowledge of the CI incident only to the authorities who have the need to know (paragraph 3-2), can appropriately respond to the situation, and if necessary, give you guidance.

3-2. Report The Incidents To The Authorities

a. All EUSA personnel must report know or suspected incidents to the nearest CI office within **24 hrs after learning of the incident**. Only Special Access Program (SAP) and Special Mission Unit personnel will report suspected CI incidents to both, their Program Security Officer and dedicated CI support offices below:

- **Theater –wide 24 Hour Hot Line:** SAEDA-99 (DSN 723 – 3299)
Commercial: 0505 723-3299
- **Uijongbu Office:** (DSN) 732-7058 / 6761 – Available during normal duty hours
After duty hours: Cell 011-695-0370
- **Seoul Office:** (DSN) 736-6387 / 3299 - Available during normal duty hours
After duty hours: Cell 011-9252-9236
- **Pyongtaek/Wonju/USAG-Humphreys Office:** (DSN) 753-8157 / 8155 –
Available during normal duty hours
After duty hours: Cell 010-3100-0171
- **Waegwan Office:** (DSN) 765-7327 / 7359 - Available during normal duty hours
After duty hours: Cell 011-9252-1439
- **Daegu Office:** (DSN) 768-6768 / 6776 – Available during normal duty hours
After duty hours: Cell 011-695-0763
- **Busan Office:** (DSN) 763-3314 / 3366 - Available during normal duty hours
After duty hours: Cell 011-9909-0993
- **Kwangju Office:** (DSN) 786-6027 / 6626 - Available during normal duty hours
After duty hours: Cell 011-9909-0027

b. If these offices are not readily available:

- (1) Report to your security manager or commander who will, with no exemption, refer reports securely and rapidly, in all cases within 24 hours to the nearest CI office.
- (2) Do not report the incident through serious incident report channels, report of surveys, security inquiries, Inspector General Reports etc. Exceptions are automated information system

intrusions and international terrorist incidents, which are separately reportable under AR 25-2, AR 190-45, and AR +525-13, respectively.

(3) Call the SAEDA99 (723-3299) Hotline in Korea, or the 1-800 CALL SPY (1-800-225-5779) Hotline in the continental US (CONUS).

(4) When assigned or traveling outside of Korea in an area without an Army CI office, and the incident is life threatening or an imminent threat to property, report immediately to the nearest Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigations, or other U.S. military intelligence or security office, Defense Attaché' Office, or Embassy/Consulate Security Office. If it is not urgent, report to your supporting CI Office at travel completion.

3-3. Contacted Personnel

If another person who wants to file a CI incident contacts you, help them contact the nearest CI office. Do not attempt to gather and report the information yourself. The CI office needs direct access to the person who has first-hand knowledge of the incident. Do not share knowledge of the incident to unauthorized third parties.

3-4. False Reporting

Personnel reporting false information to retaliate against superiors, peers, co-workers or subordinates will be subject to disciplinary or administrative action. (See article 107, U. S Code of Military Justice, (UCMJ) false official statements, and see article 134, UCMJ, threat, communicating).

Chapter 4

CI Awareness and Education

4-1. The Army as a Target

The Army is a prime, accessible target for foreign intelligence and international terrorist elements. The Army is vulnerable to espionage, sabotage, subversion, and terrorism from both within and outside the US. The "insider threat" (see Glossary, Section II) underscores the necessity for a focused and effective CI awareness, briefing, and reporting program.

4-2. Importance of DA Employee Participation

Past espionage cases have demonstrated that co-workers and supervisors of those engaging in espionage overlooked obvious indicators of involvement in espionage which, had they been reported, would have minimized the damage to national security. The knowledge, awareness, and participation of all EUSA employees are essential to the success of the Army's CI Awareness and Reporting Program.

4-3. Policy

a. All EUSA employees will receive CI Awareness and Reporting training at least annually. Personnel who handle classified or controlled unclassified information, who routinely have official contact with foreign representatives, and others who may be vulnerable to approach by a foreign intelligence service may require more frequent, individual briefings.

b. All EUSA employees will report CI related incidents (see Chapter 2) within 24 hours after becoming knowledgeable of an incident (see Chapter 3).

c. At least annually, afford Army spouses and dependents CI Awareness and Reporting training.

4-4. Training Conduct

a. General.

(1) Present CI awareness training at the unclassified level to ensure reaching the widest possible audience. When requested, provide classified training to US personnel possessing valid clearances.

(2) Ensure that briefing materials reflect recent and relevant examples of national security crimes (e.g. espionage) and are tailored to the audience and geographic area. The Army G2X will approve the terminated investigations that can be briefed along with the briefing content.

(3) Use a variety of awareness and education media to develop a strong presentation.

(4) Prepare training for large audiences, small groups, or one-on-one sessions.

(5) If linguistic support is available, provide training to EUSA employees in their native language. Consider providing a handout in the native language with the salient points of reporting CI-related incidents.

b. Trainers.

(1) SAEDA can only be trained by the following:

(a) CI Special Agent (SA)

(b) DA contractors hired by units with CI missions.

(c) DA Local National Investigators hired by 501st MI BDE with CI missions.

(2) Commands without organic CI assets will coordinate with the supporting CI office for CI Awareness and Reporting training.

(3) Commands with organic CI assets will coordinate review of their CI awareness training material with 501st MI BDE CI offices for accuracy and consistency of information.

c. Methods.

(1) In person. Only "in-person" training will satisfy the annual requirement. Training is updated and tailored to the audiences. The process of updating and tailoring the training to the customer better enables a CI SA to respond to unique situations, answer specific questions, or receive a spontaneous CI incident report subsequent to the training.

(2) Electronic/Web-based. Used only as supplemental training and does not provide credit for annual training.

(a) Technology can reach a wide audience; however, only a trained CI SA can respond to unique situations, answer specific questions, and receive a spontaneous CI incident report.

(b) Commanders will maintain a continuous level of CI awareness in their units or on their installations, by coordinating with supporting CI offices, and accessing the ACIC's on-line products (<http://acic.north-inscom.army.smil.mil/ho01.asp>).

4-5. Training Content

At a minimum, each briefing will include:

a. The fact that adversaries consider EUSA employees to be lucrative sources for classified or controlled unclassified information; and will explain how this applies to the audience.

b. The methods and techniques use by adversaries to place personnel under obligation or evoke willingness to collect information on Army activities, personnel, technologies and facilities; an explanation of the false flag approach; and actual situations which highlight these methods.

c. An explanation of anomalies, and how to identify them.

d. The types of situations and indicators to be reported as listed in Chapter 2.

e. The criminal penalties in the Uniform Code of Military Justice (UCMJ) and Title 18, United States Code; recent examples of espionage convictions; and the fact that the death penalty can be imposed for espionage conducted in peacetime.

f. That failure to report CI incidents or knowingly submitting a false report is a violation of this regulation and will result in disciplinary or administrative action and security clearance suspension.

g. The damage that espionage has caused to U.S. national security (provide recent examples or less recent that caused lasting damage).

h. The intelligence aspect of international terrorist threat and the vulnerability of EUSA employees and their family members to international terrorist acts.

i. The intelligence threat posed by non-traditional adversaries.

j. Tactics and techniques used by official foreign visitors, foreign exchange officers, and other foreign national to obtain information outside of the agreed parameters.

k. The volunteer spy, considered an "insider threat," approaches and offers their services to foreign powers. EUSA personnel must be familiar with behavioral indicators to report suspected insider threats in their organization (Table 2-1).

l. Be wary of online socializing (chat rooms, blogs, dating). The risk lies in the true identity and intent of the user to foster confidence, trust and a relationship. Anonymous online interaction has led to fraud, stalking, physical assault, identify theft, and exposure to offensive material. The use of online socialization by foreign intelligence cannot be discounted as a method to obtain Army information concerning: Army personnel, facilities, activities, training, weapons, equipment, technology, strengths, vulnerabilities, etc.

m. Posting blogs with sensitive or classified unit information which can be exploited by a foreign intelligence service.

n. Unsolicited correspondence and its link in the foreign intelligence and international terrorism collection process.

- o. The 1-800 CALL SPY (1-800-225-5779) hotline in CONUS or the OCONUS equivalent.
- p. How to respond to and report CI incidents (see Chapter 3).
- q. Research and Technology Protection, the methods of targeting, Army research and technology information and personnel working at Army Research, Development, and Acquisition programs and facilities. Define critical program information and critical research technology.

4-6. Vulnerable Personnel and Positions

Certain personnel present attractive targets or may be especially vulnerable to adversarial approach by virtue of their position, travels, duties, clearance and access level, or associations. Adversarial intelligence services have traditionally targeted and continue to target people with access to sensitive compartmented, cryptographic, and special access program information; and classified document custodians. Today, this list includes linguists and interpreters, research and development specialists; computer specialists; and others working in the scientific, technical, communications, information systems and intelligence fields.

- a. Categories of vulnerable personnel and positions.

(1) EUSA employees scheduled to travel to or through countries of counterintelligence concern (reference: current coy of DCS, G-2 Memorandum, subject: Operational Planning List (OPL) posted on the Army DCS, G2, web site – <http://www.dami.army.smil.mil>) for leave, deploying personnel, permanent change of station, or temporary duty.

(2) EUSA employees scheduled to attend scientific, technical, engineering, or other professional meetings or symposia that foreign representatives sponsor or attend, in the US or abroad.

(3) EUSA employees participating in training, education, commercial ventures, technical information sharing, or exchange programs with foreign powers.

(4) Members of agencies sponsoring foreign visitors, exchange personnel, liaison officers, and students.

(5) EUSA employees who have close and continuing relationships with relatives residing in or have other significant ties to foreign countries.

(6) Technology Project Officers, Program/Product Managers, and security managers.

(7) Foreign Disclosure Officers.

(8) Special Access Program and Special Mission Unit personnel.

(9) Personnel whose jobs require interface with foreign national dealing with weapons acquisition and Research, Development, Testing and Evaluation (RDT&E); leading edge technologies or application of those technologies to weapons or intelligence systems.

(10) Personnel serving as military attaches, or serving in US embassies or diplomatic missions abroad.

(11) Public information officers associated with RDT&E facilities.

(12) System Administrators and other key network personnel who have “administrator” level privileges on classified and sensitive Army computer networks and systems.

b. Critical Program Information Personnel. EUSA acquisition program personnel working with Critical program Information will notify their security personnel of all projected foreign travel. In addition to individual or small group CI briefings, these personnel will coordinate with EUSA Operational Protection Directorate to receive an anti-terrorism briefing prior to overseas travel.

c. Personnel with Sensitive compartmental Information (SCI) Access. EUSA employees with access to SCI will notify their security managers in advance of any official or unofficial foreign travel. Security managers will coordinate with the servicing CI unit to arrange pre-briefings and debriefings.

4-7. Conduct of Special Category Briefings (SCB) and Debriefings

a. Trainer. CI Special Agents are the preferred trainers for SCB, but because SCB occur on a more frequent basis, units with organic CI assets can conduct these briefings after a review by CI SA.

b. Method. Tailor the CI briefing to the particular risk involved, including inherent hazards and vulnerabilities, how the individual can minimize the risk, and emphasize reporting responsibilities.

c. Debriefing.

(1) Units with organic CI SA will debrief personnel identified in paragraphs 4-6a(1) through (5) as soon as possible following the travel, visit, or duty. Units without organic CI SA will coordinate with the supporting CI office to conduct the debriefing.

(2) Units without organic CI personnel will request CI assistance to conduct debriefings.

Appendix A References

Section I: Required Publications

The following publications are available at 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.

Department of Defense Instruction 5240.6, August 7, 2004 Counterintelligence Awareness, Briefing, and Reporting Programs.

Presidential Decision Directive 12, August 5, 1993 Security and Awareness and Reporting of Foreign Contacts.

White House Memorandum, August 23, 1996 Early Detection of Espionage and Other Intelligence activities through Identification and Referral of Anomalies.

Section II: Related Publications

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

AR 25-2 Information Assurance

AR 1-201 Army Inspection Policy

AR 190-45 Law Enforcement Reporting

AR 380-5 Department of the Army Information Security Program

AR 380-10 Foreign Disclosure and Contacts with Foreign Representatives

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

AR 380-381 Special Access Programs (SAPs) and Sensitive Activities

AR 381-10 U.S. Army Intelligence Activities

AR 381-14 Technical Counterintelligence

AR 381-20 The Army Counterintelligence Program

AR 525-13 Antiterrorism

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

Executive Order 12333 (amended 30 July 2008) United States Intelligence Activities

Executive Order 12829 National Industrial Security Program

Executive Order 12958 National Security Information

Department of Defense Directive 5240.02 Counterintelligence

Department of Defense Instruction 5240.16 DoD Counterintelligence Functional Services

Directive-Type Memorandum 08-007 DoD Force Protection Threat Information

Department of Defense 5220.22-M National Industrial Security Program Operating Manual Supplement

Section III: Prescribed Forms

There are no entries in this section.

Section IV: Referenced Forms

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

Glossary

Section I: Abbreviations

ACIC	Army Counterintelligence Center
ACCA	Allied CI Coordinating Authority
ACO	Allied Command Operations
ACOM	Army command
ASCC	Army service component command
ATCICA	Army Theater Counterintelligence Coordinating Authority
CI	Counterintelligence
CIR	Counterintelligence Incident Report
CONUS	Continental United States
DCS, G-2	Deputy Chief of Staff, G-2
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DPOB	Date, place of birth
DRU	Direct reporting unit
E.G.	Example gratia (Latin), "for example"
HQDA	Headquarters, Department of the Army
I.E.	Id est (Latin), "that is" or "that is to say"
INSCOM	Intelligence and Security Command
NEO	Non-combatant evacuation operations
NOFORN	Not Releasable to Foreign Nationals/Governments/Non-U.S. Citizens
OCONUS	Outside of the continental United States
RDT&E	Research, development, testing & evaluation
SA	Special Agent
SAP	Special Access Program

SAEDA	Subversion and espionage directed against the Army
SCI	Sensitive compartmented information
SCB	Special category briefing
TRADOC	Training and Doctrine Command
UCMJ	Uniform Code of Military Justice

Section II: Terms

Anomaly

Foreign power activity or knowledge, inconsistent with the expected norms that suggest prior foreign knowledge of U.S. national security information, processes or capabilities. (White House anomalies memo, DoDD 5240.02)

Antiterrorism

Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces. (AR 525-13)

Contact

Any form of meeting, association, or communication, in person, by radio, telephone, letter or other means, regardless of who started the contact or whether it was for social, official, private or other reasons. (DoDI 5240.6)

Counterintelligence

Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations, or persons or their agents, or international terrorist organizations or activities. (Executive Order 12333, amended 30 July 2008)

Counterintelligence investigations

Are conducted to prove or disprove an allegation of espionage or other intelligence activities, such as sabotage, assassination, or other national security crimes conducted by or on behalf of a foreign government, organization, or person or international terrorists. CI investigations may establish the elements of proof for prosecution or administrative actions; provide a basis for CI operations. CI investigations are conducted against individuals or groups for committing major security violations, as well as failure to follow Defense Agency and Military Department directives governing reporting contacts with foreign citizens and out-of-channel requests for defense information. CI investigations provide military commanders and policymakers with information used to eliminate security vulnerabilities and otherwise improve the security posture of threatened interests. (DoDI 5240.6)

Counterterrorism

Offensive measures taken to prevent, deter, and respond to terrorism (AR 525-13)

Espionage

The act of obtaining, delivering, transmitting, communicating, or receiving information in respect to the national defense with an intent or reason to believe that the information could be used to the

injury of the United States or to the advantage of any foreign nation and not pursuant to an international agreement duly entered into by the United States. (DoDI 5240.6)

See Title 18 U.S. Code, Chapter 37 – Espionage and Censorship

792. Harboring or concealing persons

793. Gathering, transmitting or losing defense information

794. Gathering or delivering defense information to aid foreign government

797. Publication and sale of photographs of defense installations

798. Disclosure of classified information

See Article 106a, U.S. Code of Military Justice, Espionage

See Economic Act of 1996

Force protection

Security program to protect soldiers, civilian employees, family members, information, equipment, and families in all locations and situations. (AR 525-13)

Foreign diplomatic establishment

Any embassy, consulate, or interest section representing a foreign country. (DoDI 5240.6)

Foreign power

Any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or organization composed, in major part, of any such entity or entities. (DoD 5240.1-R)

Insider threat

Acts of commission or omission, by an insider, that intentionally or unintentionally compromise the DoD's ability to accomplish its mission. Insider threats include, but are not limited to, espionage, other criminal activity, unauthorized disclosure of information, and loss or degradation of departmental resources or capabilities. (DoD CI Strategy Fiscal Years 2008-2013)

Sabotage

An act or acts with the intent to injure or interfere with, or obstruct the national defense of a country by willfully injuring, destroying or attempting to destroy any national defense or war material, premises, or utilities, to include human and natural resources. (DoD 5240.6)

See Article 108, U.S. Code of Military Justice, Destruction of Government Property

Serious incident

Any actual or alleged incident, accident, misconduct, or act, primarily criminal in nature, that, because of its nature, gravity, potential for adverse publicity, or potential consequence warrants timely notice to HQDA. (AR 190-45)

Sedition

An act or acts intending to cause the overthrow or destruction of the United States Government by force or violence, or by the assassination of any U.S. Government official. These acts include conspiracy, knowingly, or willingly advocating, abetting, advising, or teaching and duty, necessity, desirability, or propriety of overthrowing or destroying by force or violence the U.S. Government (DoDI 5240.6)

See Title 18 U.S. Code, Chapter 115 – Treason, Sedition, and Subversive Activities

2384. Seditious conspiracy

2385. Advocating overthrow of Government

See Article 94, U.S. Code of Military Justice, Mutiny or Sedition

Special Agent, Counterintelligence

Personnel holding MOS 35L, 351L, and 35E as a primary or additional secondary specialty, and civilian employees in the GG-0132 career field, who have successfully completed the Counterintelligence Special Agent Course, who are authorized to be issued Military Intelligence Badge and Credentials. (AR 381-20)

Spying

During wartime, any person who is found lurking as a spy or acting as a spy in or about any place, vessel or aircraft, within the control or jurisdiction of any of the Armed Forces or in or about any shipyard, any manufacturing or industrial plant, or any other place or institution engaged in work in aid of the prosecution of the war by the United States, or elsewhere. (DoDI 5240.6)

See Article 106, U.S. Code of Military Justice, Spying

Subversion

An act or acts inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent to interfere with, or impair the loyalty, morale, or discipline of the military forces of the United States (DoDI 5240.6)

See Title 18 U.S. Code, Chapter 115 – Treason, Sedition, and Subversive Activities

2387. Activities affecting armed forces generally

See Article 134, U.S. Code of Military Justice, Disloyal Statements

Suspicious Activity

Any behavior that is indicative of criminal activities, intelligence gathering, or other preoperational planning related to a security threat to DoD interest worldwide. (DTM 09-007)

See Article 106a, U.S. Code of Military Justice, Espionage

Terrorism

The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in pursuit of goals that are generally political, religious, or ideological. (DoDI 5240.6)

See Title 18 U.S. Code, Chapter 113B-Terrorism

2331. Definitions

2332. Criminal penalties

2332b. Acts of terrorism transcending national boundaries

2332f. Bombings of places of public use, government facilities, public transportation systems and infrastructure facilities

2339. Harboring or concealing terrorists

2339A. Providing material support to terrorists

2339B. Providing Material support or resources to designated foreign terrorist organizations

2339C. Prohibitions against the financing of terrorism

2339D. Receiving military-type training from a foreign terrorist organization

Treason

One who, owing allegiance to the United States, levies war against the United States or adheres to its enemies, giving them aid and comfort within the United States or elsewhere. It also includes one who, having knowledge of the commission of treason, conceals and does not, as soon as may be report it. (DoDI 5240.6)

See Title 18 U.S. Code, Chapter 115 – Treason, Sedition, and Subversive Activities

2381. Treason

2382. Misprision of treason

See Article 104, Aiding the Enemy

Unauthorized intrusions and unauthorized discussions on computer services

One who accesses a computer without authorization or exceeds authorized access, thereby obtaining information that has been determined to require protection for reason of national defense or foreign relations, or any restricted data, with the intent or reason to believe that such information is to be used to the injury of the United States, or to the advantage of any foreign nation; or, one having unauthorized possession of information relating to the national defense that the possessor has reason to believe could be used to the injury of the United States or to the advantage of a foreign nation, willfully communicates or transmits the same to any person not entitled to receive it over commercial on-line computer services under 18 USC 793. (DoDI 5240.6)

See Title 18 U.S. Code, Chapter 47 – Fraud and False Statements
1030. Fraud and related activity in connection with computers

Section III: Special Abbreviations and Terms

Agent of a foreign power

Any person, other than a U.S. Citizen, who ---

- Acts in the United States as an officer or employee of a foreign power or as a member of a group engaged in preparing for or conducting international terrorist activities.
- Acts for or on behalf of a foreign power that engages in clandestine intelligence activities in the United States contrary to the interest of the United States, if the circumstances of the person's presence in the United States indicate that he or she may engage in such activities in the United States, or if the person knowingly aids or abets any person in conducting such activities or knowingly conspires with any person to engage in such activities.

Any person who ---

- For or on behalf of a foreign power, knowingly engages in clandestine intelligence-gathering activities that involve or may involve a violation of the criminal statutes of the United States.
- Pursuant to the direction of an intelligence service or network of a foreign power, and for or on behalf of that power, knowingly engages in any other clandestine intelligence activities that involve or are about to involve a violation of the criminal statutes of the United States.
- Knowingly prepares for or engages in sabotage or terrorism for or on behalf of a foreign power.
- Knowingly aids or abets any person in the conduct of the activities described above or knowingly conspires with any person to engage in the activities described above.

Countries of current concern

Foreign powers of U.S. National concern due to targeted intelligence collection against the Army, internal unrest or war, terrorist sponsorship, efforts to obtain Army-related technology without authorization, or efforts to develop weapons of mass destruction.

EUSA employee

Military (active and reserve), civilian and foreign nationals employed by the Department of the Army, and DA contractors.

False Flag approach

An intelligence officer or agent represents himself as a person of another nationality in order to foster trust and lessen suspicion about the contact.

Supporting CI office

A CI office assigned responsibility for supporting a command, facility, program, etc. For DA contractors, the supporting CI office is normally the Federal Bureau of Investigation.

Unauthorized disclosure

Intentionally conveying classified documents, information, or material to any unauthorized person (one without the required clearance, access, and need to know).

Unsolicited correspondence

Unsolicited requests for information from a foreign national, which may range from direct inquiries by phone, email, fax or letter to questionnaires in which the recipient is asked to provide seemingly innocuous data. Typical requests for additional information after a public presentation, suggestions for mutual research, requests for survey participation, etc. The actual purpose may be to identify by name and position any individual who might be targeted later by a foreign intelligence service, and to elicit targeted information not readily obtainable by other means.