

Army Regulation 381-12

Military Intelligence

Threat Awareness and Reporting Program

**Headquarters
Department of the Army
Washington, DC
4 October 2010**

UNCLASSIFIED

SUMMARY of CHANGE

AR 381-12

Threat Awareness and Reporting Program

This major revision, dated 4 October 2010--

- o Changes the title of the regulation from Subversion and Espionage Directed Against the U.S. Army to Threat Awareness and Reporting Program (cover).
- o Adds the Director, Army G-2X as the primary staff element responsible for establishing and maintaining a centralized system of control for the reporting of threat incidents and follow-on counterintelligence investigations (para 1-5a).
- o Requires threat-awareness training be included in courses of instruction at the U.S. Army Training and Doctrine Command schools and centers (para 1-7a).
- o Mandates threat-awareness training and reporting requirements be included in unit command inspection programs (para 1-10g).
- o Requires counterintelligence units to submit counterintelligence incident reports to the Director, Army G-2X within 72 hours after acquiring information about the incident from the original source or others knowledgeable (paras 1-12f and 5-1c).
- o Adds policy for contractors with security clearances to comply with threat-awareness reporting requirements (para 1-14b).
- o Defines standards for the content of threat-awareness briefings (para 2-5).
- o Identifies personnel who are vulnerable to exploitation by foreign intelligence and international terrorist organizations and requires they receive special threat-awareness training (paras 2-6 and 2-7).
- o Expands the list of reportable threat-related incidents and situations to include indications of potential international terrorist related insider threat activity (chap 3).
- o Organizes the behaviors that may be exhibited by a person engaging in espionage; includes a table listing the indicators of potential terrorist associated insider threats directed against the Army, DOD, or the United States and includes a table listing the indicators of extremist activity that may pose a threat to DOD or disrupt U.S. military operations (tables 3-1, 3-2, and 3-3).
- o Requires expeditious reporting of threat activity and behavioral indicators to counterintelligence units (paras 4-1d and 4-2b and c).


Military Intelligence

Threat Awareness and Reporting Program

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 major revision.

Summary. This regulation implements DODI 5240.6. It provides policy and responsibilities for threat awareness and education and establishes a requirement for DA personnel to report any incident of known or suspected espionage, international terrorism, sabotage, subversion, theft or diversion of military technology, information systems intrusions, and unauthorized disclosure of classified information, among others.

Applicability. This regulation applies to the active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to the following: Department of the Army civilian

personnel; DOD contractor personnel with security clearances for their briefing and reporting requirements as specified under EO 12829; and foreign nationals employed by the DA. The applicability of this regulation to local national employees and contractors employed by Army agencies in overseas areas will be governed by Status of Forces Agreements and applicable treaties between the United States and host countries. During mobilization or national emergency, this regulation remains in effect without change.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G-2. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent 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 expected benefits and must include 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 internal control process. This regulation contains internal control provisions and identifies key management controls that must be evaluated (see appendix C).

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, 1000 Army Pentagon, 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, 1000 Army Pentagon, Washington, DC 20310-1000.

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 U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1 Introduction, page 1

Section 1

General, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

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

*This regulation supersedes AR 381-12, dated 15 January 1993.

Contents—Continued

Section II

Responsibilities, page 1

Deputy Chief of Staff, G-2 • 1-4, *page 1*

Director, Army G-2X • 1-5, *page 1*

Commander, U.S. Army Reserve Command and Chief, National Guard Bureau • 1-6, *page 1*

Commander, U.S. Army Training and Doctrine Command • 1-7, *page 2*

Commanders, Army commands, Army service component commands, and direct reporting units • 1-8, *page 2*

Commander, U.S. Army Intelligence and Security Command • 1-9, *page 2*

All Army commanders • 1-10, *page 2*

Commander, 650th Military Intelligence Group • 1-11, *page 3*

Unit commanders with counterintelligence personnel assigned or attached • 1-12, *page 3*

All DA personnel • 1-13, *page 3*

Contractors and contract management personnel • 1-14, *page 4*

Chapter 2

Threat Awareness and Education, page 4

Section I

General, page 4

Army as a target • 2-1, *page 4*

Importance of DA personnel participation • 2-2, *page 4*

Threat awareness policy • 2-3, *page 4*

Section II

Threat-Awareness Training, page 4

Conduct of threat-awareness training • 2-4, *page 4*

Content of threat awareness training • 2-5, *page 5*

Section III

Special Threat-Awareness Training, page 5

Vulnerable personnel and positions • 2-6, *page 5*

Conduct of special threat-awareness briefings and debriefings • 2-7, *page 6*

Section IV

General Counterintelligence Support, page 6

Publicizing threat awareness • 2-8, *page 6*

Supplemental training • 2-9, *page 6*

Chapter 3

Reporting Requirements, page 7

Reportable threat-related incidents • 3-1, *page 7*

Behavioral threat indicators • 3-2, *page 8*

Additional matters of counterintelligence interest • 3-3, *page 8*

Chapter 4

Reporting Procedures, page 11

Individual response • 4-1, *page 11*

Reporting the incident • 4-2, *page 11*

Additional reporting requirements • 4-3, *page 11*

Fabricated reporting • 4-4, *page 12*

Obstruction of reporting • 4-5, *page 12*

Chapter 5

Counterintelligence Unit Reporting Policy and Procedures, page 12

Receipt of threat reports from DA personnel • 5-1, *page 12*

Contents—Continued

Other considerations • 5–2, *page 12*

Chapter 6

Assessment of the Threat Awareness and Reporting Program, *page 12*

Purpose • 6–1, *page 12*

Counterintelligence unit responsibility • 6–2, *page 12*

Army service component command, Army commands, and direct reporting unit responsibility • 6–3, *page 13*

Appendixes

A. References, *page 14*

B. Counterintelligence Incident Report Format, *page 16*

C. Internal Control Evaluation Certification, *page 18*

Table List

Table 3–1: Indicators of espionage, *page 9*

Table 3–2: Indicators of potential (international) terrorist-associated insider threats, *page 10*

Table 3–3: Indicators of extremist activity that may pose a threat to DOD or disrupt U.S. military operations, *page 10*

Glossary

Chapter 1 Introduction

Section I General

1–1. Purpose

This regulation establishes policy, responsibilities, and procedures for the Army's Threat Awareness and Reporting Program (TARP). This regulation includes a specific definition of the threat based on the activities of foreign intelligence, foreign adversaries, international terrorist organizations, extremists, and behaviors that may indicate that Department of the Army (DA) personnel pose a danger to the Army, Department of Defense (DOD), or the United States. The primary focus of this regulation is to ensure that DA personnel understand and report potential threats by foreign intelligence and international terrorists to the Army. Threat awareness and education training is designed to ensure that DA personnel recognize and report incidents and indicators of attempted or actual espionage, subversion, sabotage, terrorism or extremist activities directed against the Army and its personnel, facilities, resources, and activities; indicators of potential terrorist associated insider threats; illegal diversion of military technology; unauthorized intrusions into automated information systems; unauthorized disclosure of classified information; and indicators of other incidents that may indicate foreign intelligence or international terrorism targeting of the Army.

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.

Section II Responsibilities

1–4. Deputy Chief of Staff, G–2

The DCS, G–2 will—

- a. As the senior intelligence officer of the Army, exercise Army staff responsibility for policy and procedures related to threat awareness and reporting.
- b. Implement DOD and higher level counterintelligence (CI) policy; develop, approve, and publish Army threat awareness and reporting policy and procedures; and provide interpretation of policy, as required.
- c. Oversee the implementation of the TARP and ensure its effectiveness as an element of the Army's overall CI effort.
- d. Establish policy and guidelines for the processing, investigation, and disposition of matters and incidents reported by Army personnel under this regulation, as appropriate.
- e. Ensure that the Army leadership is aware of significant threat and other CI related incidents.

1–5. Director, Army G–2X

The Director, Army G–2X will—

- a. Through the Army Counterintelligence Coordinating Authority (ACICA), maintain a centralized system of control and coordination of CI incident reporting and any resulting CI investigations and operations worldwide.
- b. Ensure that the TARP is implemented as a priority for the development of CI leads.
- c. Assess the effectiveness of threat awareness and reporting in accordance with chapter 6.
- d. Maintain a database which contains a concise synopsis of CI incident reports (CIR) and follow on CI investigations.
- e. Ensure that key information related to CIR is entered into an approved DOD CI information system, such as PORTICO.
- f. Ensure that data on CI incident reporting is shared with the Army Counterintelligence Center (ACIC), which is responsible for CI analysis in the Army.
- g. Serve as the approval authority for the release of information from closed CI investigations for use in threat awareness briefings.

1–6. Commander, U.S. Army Reserve Command and Chief, National Guard Bureau

These officials will—

- a. Ensure that reserve component CI agents provide threat awareness training to U.S. Army Reserve (USAR) and Army National Guard (ARNG) personnel at least annually, as required by this regulation.

b. Ensure that reserve component CI units have access to CI analysis and that current, relevant, and appropriate foreign intelligence and international terrorist threat data is used for threat awareness and training.

1-7. Commander, U.S. Army Training and Doctrine Command

The commander, TRADOC will—

a. Develop and implement, in coordination with supporting CI offices, threat-awareness training at TRADOC schools and training centers. The objective of this training is to prepare students to apply their awareness of threat reporting requirements when they arrive at their first assignments.

b. Ensure that brigade and battalion level commanders receive threat-awareness training in Army precommand courses to familiarize them with command and individual responsibilities and the role of the supporting CI unit.

c. Ensure sergeants major receive threat-awareness training in their respective leadership courses to familiarize them with the program, with command and individual responsibilities, and the role of the supporting CI unit.

1-8. Commanders, Army commands, Army service component commands, and direct reporting units

Commanders of ACOMs, ASCCs, and DRUs will—

a. Establish a threat-awareness program and ensure that all DA personnel receive awareness training annually, conducted either by the supporting CI unit or organic CI agents, if available.

b. Ensure that all incidents specified in chapter 3 are reported according to the instructions in chapter 4 and that there is command emphasis on the importance of threat reporting.

c. Through the Army Theater Counterintelligence Coordinating Authority (ATCICA) or organic CI staff element, whichever is appropriate, manage and provide oversight of the TARP.

1-9. Commander, U.S. Army Intelligence and Security Command

The commander, INSCOM will—

a. Implement and maintain a robust, professional, and effective TARP through subordinate commands in support of Army units worldwide.

b. Ensure that assigned or attached CI agents respond to those threat-related incidents, behavioral indicators, and other matters of CI interest specified in chapter 3 when such matters are reported by DA personnel to Army CI.

c. Ensure that CIR are submitted by assigned or attached CI agents in accordance with the policy and procedures in this regulation.

d. Ensure that subordinate CI unit commanders and supervisors do not obstruct or impede the submission of CIR.

e. Assist supported units in developing programs to publicize the importance of threat reporting.

f. Ensure that threat-awareness training is presented in a professional and knowledgeable manner and that the content of briefings is current and relevant.

g. As appropriate, conduct follow-on CI investigations of CI incidents at the direction of the ACICA as specified in AR 381-20.

h. Conduct analysis of CIR and CI investigations to assist commanders in developing security countermeasures programs, when appropriate.

i. Develop assessments of trends in foreign intelligence and international terrorist activity for use in threat-awareness training.

j. Produce an annual report on the foreign intelligence and international terrorist threat to the Army.

1-10. All Army commanders

Army commanders at all levels will—

a. Ensure that those threat incidents, behavioral indicators, and other CI matters identified in chapter 3 are properly reported in accordance with the instructions in chapter 4.

b. Place command emphasis on the importance of prompt threat reporting and the possible disciplinary actions under the Uniform Code of Military Justice (UCMJ) or adverse personnel actions for failure to report those incidents specified in paragraph 3-1.

c. Incorporate threat awareness training into unit training schedules and ensure that all DA personnel, including Army contractors with security clearances, receive annual threat awareness training by a CI agent or other trainer as specified in paragraph 2-4*b*.

d. Identify those personnel who should receive special threat-awareness briefings, as indicated in paragraph 2-6, and ensure they are scheduled for briefing at the request of CI agents.

e. Ensure that knowledge of CI incidents is limited by reporting incidents directly to the supporting CI office, whenever possible. This restriction preserves the integrity of any ensuing investigation.

f. Monitor the unit threat awareness program to ensure that—

(1) Training is conducted by CI trainers as specified at paragraph 2-4*b*.

(2) Assigned personnel cooperate with CI agents in the collection of information on threat-related incidents and the briefings and debriefings specified at paragraphs 2–6 and 2–7.

g. Inspect compliance with the threat awareness and reporting requirements of this regulation in unit command inspection programs (see app C).

h. Maintain a continuous level of threat awareness in their units and on their installations through coordination with supporting CI offices and by accessing online foreign intelligence and international terrorist threat products produced by the ACIC (available at <http://acic.north-inscom.army.smil.mil/ho01.asp>).

1–11. Commander, 650th Military Intelligence Group

The commander, 650th MI Group will—

a. Implement the threat awareness program to supported organizations, personnel, facilities, and programs in the North Atlantic Treaty Organization, Allied Command Operations, Allied Command Transformation; and U.S. personnel assigned to or supporting the North Atlantic Treaty Organization, Allied Command Operations, and Allied Command Transformation.

b. Assist supported units in developing programs to publicize the importance of threat awareness and reporting.

c. Ensure that threat awareness briefings are presented in a professional and knowledgeable manner in accordance with this regulation. Ensure that briefings include information from recent espionage, international terrorism, or other national security related investigations.

d. Through the Allied CI Coordinating Authority (ACCA), manage and control CI activities, including the oversight and assessment of the TARP.

1–12. Unit commanders with counterintelligence personnel assigned or attached

These commanders will—

a. Support all Army commanders in the unit's area of responsibility with a TARP.

b. Ensure that the content of threat awareness training includes those items identified at paragraph 2–5 and that CI trainers are following these guidelines.

c. Ensure that the content of threat awareness training is tailored appropriately to the mission, geographic location, and degree of potential international terrorist or foreign intelligence threat to the organization receiving training.

d. Coordinate with supported commands to identify those personnel who require special threat-awareness training and conduct the briefings and debriefings of these personnel, as appropriate.

e. Ensure that Army personnel reporting CI incidents are interviewed about the details of the incident as soon as possible.

f. Submit CIR within 72 hours of the incident being reported to the CI unit.

(1) Continental United States (CONUS) units will submit CIR directly to the ACICA with information copies to the appropriate chain of command.

(2) Units outside the continental United States (OCONUS) will submit CIR directly to the ACICA with information copies to the appropriate ATCICA and chain of command.

(3) Units deployed in support of combatant commanders will submit CIR directly to the ACICA with information copies to the appropriate CI coordinating authority (CICA) and chain of command.

g. As specified in paragraph 6–2, produce a quarterly report on the threat awareness training presented to supported organizations during the previous quarter. This report will be used by the Director, Army G–2X as part of a broader effort to assess and evaluate the effectiveness of CI in the Army.

h. When preparing for deployment in support of combat commanders, develop procedures and mechanisms to ensure that supported units are able to securely and quickly report threat related incidents, behavioral indicators, and other matters of CI interest.

i. In a deployed environment, ensure that supported commands are aware of how and to whom to report threat related incidents.

j. Coordinate with security managers and S–2 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 reports from DA personnel.

1–13. All DA personnel

DA personnel will—

a. Be knowledgeable of those reportable threat-related incidents and behavioral indicators in chapter 3.

b. Be knowledgeable of how to contact the supporting Army CI office.

c. Follow the procedures in paragraph 4–2 for reporting the incident.

d. Cooperate with or assist CI agents on the conduct of their official duties.

e. Not discuss the details of the incident that they have reported to anyone else unless authorized by the CI agent. Any command briefings or notifications that may be required will be accomplished by the CI agent.

1–14. Contractors and contract management personnel

Contractors and contract management personnel will proceed as follows:

a. Army contracting officers or contracting officer representatives will ensure that threat awareness and reporting requirements are included in future classified contracts or on DD Form 254 (Department of Defense Contract Security Classification Specification), as appropriate.

b. The contracting officers or contracting officer representatives will ensure Army contractors with security clearances comply with threat awareness and reporting requirements specified by this regulation.

c. Persons employed by Army contractors will report threat-related incidents, behavioral indicators, and other matters of CI interest specified in chapter 3, to the facility security officer, the nearest military CI office, the Federal Bureau of Investigation, or the Defense Security Service.

Chapter 2 Threat Awareness and Education

Section I General

2–1. Army as a target

a. The Army is a prime target for foreign intelligence and international terrorist elements. The Army faces the threat of espionage, sabotage, subversion, and international terrorism from within and OCONUS.

b. The Army also faces threats from persons on the inside (the insider threat), those with placement and access in an organization who may compromise the ability of the organization to accomplish its mission through espionage, acts of terrorism, support to international terrorist organizations, or unauthorized release or disclosure of classified or sensitive information. The potential of the insider threat to cause serious damage to national security underscores the necessity for a focused and effective TARP.

2–2. Importance of DA personnel participation

Past espionage cases and acts of international terrorism that have targeted Army personnel and facilities have demonstrated that coworkers, associates, friends, and supervisors of those engaging in espionage or terrorist activity have overlooked indicators of potential threats to the Army which, had they been reported, would have minimized the damage to national security or saved the lives of DA personnel. The knowledge, awareness, and participation of all DA personnel in threat awareness and reporting is essential to the success of the Army's accomplishment of its warfighting mission and in protecting the lives of Soldiers.

2–3. Threat awareness policy

a. All DA personnel will undergo threat-awareness training at least annually.

b. Personnel who handle classified information; work in intelligence disciplines; routinely have official contact with foreign representatives; or have foreign connections or associations may be more vulnerable to approach by a foreign intelligence service or influence from an international terrorist organization, and may require more frequent briefings on an individual basis. Policy on the conduct of special threat-awareness training is in paragraphs 2–6 and 2–7.

c. DA personnel will report those incidents or behavioral indicators as detailed in chapter 3. Instructions for reporting are outlined in chapter 4.

Section II Threat-Awareness Training

2–4. Conduct of threat-awareness training

a. General.

(1) Threat-awareness training will be presented at the unclassified level to ensure reaching the widest possible audience. When requested, classified training may be provided to DA personnel possessing the appropriate clearance.

(2) CI units will ensure that briefing materials reflect recent and relevant examples of national security crimes (for example, espionage and international terrorism) and are tailored to the audience and geographic area.

(3) Briefers will use a variety of awareness and education media to develop a strong and professional presentation.

(4) Briefers may prepare training for large audiences, small groups, or individuals.

(5) If linguistic support is available, it is preferable to provide training to DA personnel in their native language. Consider providing a handout in the native language with the salient points of reporting threat-related incidents.

b. Trainers.

(1) Threat awareness training will be conducted only by—

- (a) CI special agents.
 - (b) Army contractors hired by units with a CI mission.
 - (c) Local national investigators hired by OCONUS units with a CI mission.
- (2) Commands without organic CI assets will coordinate with the supporting CI office to arrange for the conduct of training.
- (3) Commands with organic CI elements may coordinate with supporting CI offices in order to acquire training materials which are recent and relevant.

c. Methods.

(1) *Live training.* Live training, with the CI agent making the presentation to a live audience, is the preferred means of delivering threat awareness training. This allows the trainer to tailor the training to the needs of the audience; the CI agent to respond to unique situations and answer specific questions; Soldiers to report threat-related incidents to an agent while the agent is available; and the audience to know the identity of the person to whom incidents should be reported.

(2) *Alternative training.* In those instances where live training is not possible, such as in deployed theaters of operation, CI units may, in coordination with appropriate commanders, develop alternative means to conduct threat awareness training and meet the requirements of this regulation. This training may be conducted online, through the use of video equipment, or other electronic media.

2-5. Content of threat awareness training

At a minimum, each briefing will include—

- a.* The fact that foreign adversaries consider DA personnel to be lucrative sources for defense information and attractive targets of terrorism.
- b.* The methods and techniques used by foreign 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.* The methods used by international terrorists to target Army personnel and the vulnerabilities that terrorists exploit to harm the Army.
- d.* The means by which an insider threat may exploit knowledge of a unit's plans and intentions to provide operational information to the enemy, and the means which an insider may employ to target DA personnel.
- e.* The types of situations and indicators of both espionage and international terrorism that should be reported.
- f.* The provisions of the UCMJ and Title 18, United States Code (USC) related to national security crimes; recent examples of espionage convictions; and the fact that the death penalty may be imposed for espionage conducted in peacetime.
- g.* That failure to report those threat incidents specified in paragraph 3-1 is a violation of this regulation and may result in disciplinary or adverse administrative action.
- h.* The damage that espionage and the terrorist insider have caused to U.S. national security using recent examples.
- i.* The intelligence threat posed by friendly foreign countries.
- j.* Tactics and techniques used by official foreign visitors to Army installations to obtain information to which they are not authorized access. Official foreign visitors include foreign liaison officers and foreign exchange officers.
- k.* The need to be cautious in the use of online social networking sites (chat rooms, blogs, and online dating sites) and the ways in which foreign intelligence has exploited these sites to assess Army personnel for potential future recruitment or to acquire classified or sensitive unclassified information.
- l.* Cautions against posting blogs with information about a person's military duties, military plans and intentions, or any other information which may be exploited by a foreign intelligence service or international terrorist organization.
- m.* Unsolicited correspondence and how it is used by foreign intelligence and international terrorist organizations.
- n.* Foreign intelligence interest in critical military technology and the methods of targeting Army personnel working in research, development and acquisition (RDA) programs and facilities.
- o.* How to respond to and report threat-related incidents.
- p.* The 1-800 CALL SPY (1-800-225-5779) Hotline in CONUS or the OCONUS equivalent.
- q.* Use of the Web-based threat reporting system available at Army Knowledge Online.

Section III Special Threat-Awareness Training

2-6. Vulnerable personnel and positions

Certain DA personnel may be especially vulnerable to exploitation by foreign intelligence or international terrorism. Foreign intelligence services have traditionally targeted and continue to target DA personnel with access to sensitive compartmented information, cryptographic, and Special Access Program (SAP) information. Persons involved in research and development of critical technology; information operations specialists; persons working in the scientific,

technical, communications, and intelligence fields; and personnel working as interpreters and linguists are also especially vulnerable. The CI units will coordinate with supported unit security managers to identify potentially vulnerable personnel and provide them special threat-awareness training, either one-on-one or in small groups. Security managers who are aware of specially vulnerable personnel scheduled to travel as indicated in paragraph 2–6a will coordinate with the servicing CI unit to arrange pretravel threat briefings and debriefings. The following personnel should receive special threat awareness training:

- a. DA personnel scheduled to travel to or through countries with a high intelligence or terrorist threat level as identified by Defense Intelligence Agency (DIA). To access information on worldwide threat levels, go to the DIA homepage on the secure internet protocol router (SIPR). Under DIA Analysis, click on the “Combating Terrorism Knowledge Base.” For additional information, under Resources, click on “Worldwide Threat Levels.” DA personnel with access to SAP information will notify their security managers in advance of any official or unofficial foreign travel.
- b. DA personnel scheduled to attend scientific, technical, engineering, or other professional meetings or symposia that representatives from foreign countries sponsor or attend, whether in the U.S. or abroad.
- c. DA personnel participating in training, education, commercial ventures, technical information sharing, or exchange programs with foreign governments or organizations.
- d. Members of agencies sponsoring or meeting with foreign visitors, foreign exchange personnel, foreign liaison officers, and foreign students.
- e. DA personnel who have close and continuing relationships with relatives or others residing in, who have foreign business connections or financial interests in, or who have other significant ties to foreign countries.
- f. System administrators and other key information network personnel who have administrator-level privileges on classified or unclassified Army information systems.
- g. Personnel whose jobs require interface with foreign governments or businesses regarding RDA activities or critical military technology.
- h. Persons with access to SAP information and persons assigned to special mission units (SMU).
- i. Personnel serving as military attachés or serving in U.S. embassies or diplomatic missions abroad.

2–7. Conduct of special threat-awareness briefings and debriefings

- a. Special threat awareness briefings will be presented to those personnel identified in paragraph 2–6, above, and will either be conducted one-on-one with the individual concerned or in small groups. These briefings will be conducted by CI agents.
- b. The CI agent will tailor the briefing to the particular risk or threat involved, including methods the person may use to minimize the risk, and will place special emphasis on reporting responsibilities.
- c. The CI debriefings will be conducted as soon as feasible following completion of travel, duty, or visit to a foreign country, or attendance at a conference with foreign personnel.
- d. If information reportable in accordance with chapter 3 is disclosed during the debriefing, CI agents will submit a CIR.

Section IV

General Counterintelligence Support

2–8. Publicizing threat awareness

As an adjunct to threat awareness training, CI units are encouraged to use all forms of DOD Media to promote threat awareness. DOD Media consist of, but are not limited to, Armed Forces Network radio television spots, regional newspaper, newsletters, posters, and military Intranet.

- a. Before making threat awareness information available in public media, including speeches, radio or television interviews, print media, Internet, or other communications media, the CI unit will coordinate with the unit or installation public affairs officer for review.
- b. The first O5 or equivalent in the CI unit chain of command, unless further delegated, will serve as the approval authority for any publicity initiative involving threat awareness. Intelligence contingency funds will not be used for this purpose. These publicity initiatives are not a replacement for the annual threat awareness training.

2–9. Supplemental training

Units may conduct supplemental threat awareness training in addition to the annual training requirement. Supplemental training may be conducted live by a CI agent or through the use of Web-based, video, or other media. Situations which may indicate the need for additional threat awareness training include, but are not limited to the following:

- a. Mass unit in-processing or outprocessing.
- b. Preparation for deployment or redeployment.
- c. Preparation for special missions or activities.
- d. Support to noncombatant evacuation operations and exercises.

- e. Military training exercises.
- f. Force protection exercises.
- g. General unit refresher training.

Chapter 3 Reporting Requirements

3-1. Reportable threat-related incidents

All DA personnel will report the incidents described below in accordance with the reporting instructions in chapter 4. Personnel subject to the UCMJ who fail to comply with the requirement to report these incidents are subject to punishment under UCMJ, as well as to adverse administrative or other adverse action authorized by applicable provisions of the USC or Federal regulations. Personnel not subject to the UCMJ who fail to comply with the provisions of this paragraph are subject to adverse administrative action or criminal prosecution as authorized by applicable provisions of the USC or Federal regulation. DA personnel will report the following:

a. Attempts by anyone, regardless of nationality, to obtain or acquire unauthorized access to classified or 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 (including electronic correspondence), or automated systems intrusions.

b. Contact with an individual, regardless of nationality, under circumstances that suggest a DA person may be the target of attempted recruitment by a foreign intelligence service or international terrorist organization.

c. Any DA personnel who are engaging in, or have engaged in, actual or attempted acts of treason, spying, or espionage.

d. Any DA personnel who are in contact with persons known or suspected to be members of or associated with foreign intelligence, security, or international terrorist organizations. This does not include contacts that DA personnel have as part of their official duties.

e. Any DA personnel who have contact with anyone possessing information about planned, attempted, suspected, or actual international terrorism, espionage, sabotage, subversion, or other intelligence activities directed against the Army, DOD, or the United States.

f. Any DA personnel who are providing financial or other material support to an international terrorist organization or to someone suspected of being a terrorist.

g. Any DA personnel who are associated with or have connections to known or suspected terrorists.

h. Any DA personnel who are in contact with any official or citizen of a foreign country when the foreign official or citizen—

(1) Exhibits excessive knowledge of or undue interest in DA personnel or their duties which is beyond the normal scope of friendly conversation.

(2) Exhibits undue interest in the research and development of military technology; military weapons and intelligence systems; or scientific information.

(3) Attempts to obtain classified or unclassified information.

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

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

i. Incidents in which DA personnel or their Family members traveling to or through foreign countries are contacted by persons who represent a foreign law enforcement, security, or intelligence organization and—

(1) Are questioned about their duties.

(2) Are requested to provide classified or unclassified information.

(3) Are threatened, coerced, or pressured in any way to cooperate with the foreign official.

(4) Are offered assistance in gaining access to people or locations not routinely afforded Americans.

j. Known or suspected unauthorized disclosure of classified information to those not authorized to have knowledge of it, including leaks to the media. (The Army requirements to report compromises or conduct inquiries as specified in AR 380-5 also apply to these incidents.)

k. Any DA personnel who remove classified information from the workplace without authority or who possess or store classified information in unauthorized locations.

l. Attempts to encourage military or civilian personnel to violate laws or disobey lawful orders or regulations for the purpose of disrupting military activities (subversion).

m. Any DA personnel participating in activities advocating or teaching the overthrow of the U.S. Government by force or violence, or seeking to alter the form of government by unconstitutional means (sedition).

n. Known or suspected intrusions by a foreign entity into classified or unclassified information systems.

o. Incidents in which authorized users of government information systems attempt to gain unauthorized access or attempt to circumvent security procedures or elevate their access privileges without approval.

p. Transmission of classified or sensitive, unclassified military information using unauthorized communications or computer systems.

q. Any situation involving coercion, influence, or pressure brought to bear on DA personnel through Family members residing in foreign countries.

r. Any DA personnel who defect to another nation, attempt or threaten to defect, and then return to military control of U.S. military and civilian defectors.

3–2. Behavioral threat indicators

The DA personnel should report, in accordance with the instructions in chapter 4, information regarding DA personnel who exhibit any of the behaviors that may be associated with a potential espionage or international terrorist threat and those associated with extremist activity that may pose a threat to the Army, or DOD, or disrupt U.S. military operations as described in the tables 3–1, 3–2, and 3–3, below. A single indicator by itself does not necessarily mean that a person is involved in activities that threaten the Army, DOD, or the United States; however, reporting the behavior to the supporting CI office will allow CI agents to appropriately assess the threat potential or, if appropriate, refer the incident to another agency.

3–3. Additional matters of counterintelligence interest

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

a. Unauthorized or unexplained absence of DA personnel who, within 5 years preceding their absence, had access to TOP SECRET, cryptographic, special access program, sensitive compartmented, or Critical Nuclear Weapons Design information, or an assignment to an SMU. (This report is in addition to the immediate report to the Provost Marshal required by AR 630–10.)

b. Actual or attempted suicide of DA personnel with access to classified information, when the member has or had an intelligence background, was assigned to an SMU, or had access to classified information within the last year.

c. Any DA personnel or their Family members who are detained in a foreign country or captured by a foreign adversary or international terrorist organization.

d. Impersonation of military intelligence personnel, or the unlawful possession or use of Army intelligence identification, such as badges and credentials.

e. Intentional compromise of the identity of U.S. intelligence personnel engaged in foreign intelligence and counterintelligence activities.

f. Incidents in which foreign countries offer employment to U.S. personnel in the design, manufacture, maintenance, or employment of weapons of mass destruction, or other critical technology fields.

g. Known or suspected compromise or illegal diversion of U.S. military critical technology or weapon systems by anyone on behalf of or for the benefit of a foreign power.

h. Incidents in which U.S. Government-owned laptop computers or other portable computing and data storage devices are known or suspected to have been tampered with while the user was traveling in a foreign country. Tampering often occurs when the device is left unattended in a hotel room. If tampering is suspected, refrain from turning the device on or using it and provide it to the supporting CI office immediately upon return.

i. Implied threats to or about persons protected by the U.S. Secret Service (see AR 381-20).

j. Discovery of a suspected listening device or other technical surveillance device. Do not disturb the device or discuss the discovery of it in the area where the suspected device may be located and immediately report its presence in-person or via secure communications to the security manager or nearest CI office. (See AR 381–14 (C)).

k. Any DA personnel interacting with persons in online social networking sites who experience—

(1) Requests to obtain classified or unclassified military information.

(2) A query about their military duties, where they are stationed, or what they have access to.

(3) An attempt to place them under obligation through special treatment, favors, gifts, money, or other means.

(4) An invitation to meet in-person at a designated location.

l. Communications security incidents that are the result of deliberate security compromises; in which there are indications of foreign intelligence or international terrorist involvement; or in which the person or persons involved exhibit behaviors that may be associated with espionage or international terrorism as specified in tables 3–1, 3–2, and 3–3.

**Table 3-1
Indicators of espionage**

Behaviors	Indicators
Foreign influence or connections	<ul style="list-style-type: none"> • Frequent or regular contact with foreign persons from countries which represent an intelligence or terrorist threat to the United States. • Unauthorized visits to a foreign embassy, consulate, trade, or press office, either in CONUS or OCONUS. • Unreported contact with foreign government officials outside the scope of one's official duties. • Business connections, property ownership, or financial interests internal to a foreign country. • Sending large amounts of money to persons or financial institutions in foreign countries. • Receiving financial assistance from a foreign government, person, or organization.
Disregard for security practices	<ul style="list-style-type: none"> • Discussing classified information in unauthorized locations. • Improperly removing security classification markings from documents and computer media. • Requesting witness signatures on classified document destruction forms when the witness did not actually observe the destruction. • Bringing unauthorized cameras, recording or transmission devices, laptops, modems, electronic storage media, cell phones, or software into areas where classified data is stored, discussed, or processed. • Repeated involvement in security violations. • Removing, downloading, or printing classified data from DOD computer systems without approval to do so.
Unusual work behavior	<ul style="list-style-type: none"> • Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities. • Attempts to obtain information for which the person has no authorized access or need to know. • Using copy, facsimile machines, document scanners, or other automated or digital equipment to reproduce or transmit classified material which appears to exceed job requirements. • Repeatedly performing non required work outside of normal duty hours, especially if unaccompanied. • "Homesteading" (requesting tour of duty extensions in one assignment or location), when the assignment offers significant access to classified information. • Manipulating, exploiting, or hacking government computer systems or local networks to gain unauthorized access.
Financial matters	<ul style="list-style-type: none"> • Unexplained or undue affluence without a logical income source. • Free spending or lavish display of wealth which appears beyond normal income. • A bad financial situation that suddenly reverses, opening several bank accounts containing substantial sums of money, or the repayment of large debts or loans. • Sudden purchases of high value items where no logical income source exists. • Attempts to explain wealth as an inheritance, gambling luck, or a successful business venture, without facts supporting the explanation.
Foreign travel	<ul style="list-style-type: none"> • Frequent or unexplained trips of short duration to foreign countries. • Travel that appears unusual or inconsistent with a person's interests or financial means.
Undue interest	<ul style="list-style-type: none"> • Persistent questioning about the duties of coworkers and their access to classified information, technology, or information systems. • An attempt to befriend or recruit someone for the purpose of obtaining classified or unclassified information.
Soliciting others	<ul style="list-style-type: none"> • Offers of extra income from an outside venture to those with sensitive jobs or access. • Attempts to entice coworkers into criminal situations which could lead to blackmail or extortion. • Requests to obtain classified information to which the requestor is not authorized access.

Table 3–2
Indicators of potential (international) terrorist-associated insider threats

- Advocating support for terrorist organizations or objectives.
 - Expressing hatred of American society, culture, government, or principles of the U.S. Constitution.
 - Advocating the use of unlawful violence or force to achieve goals that are political, religious, or ideological in nature.
 - Sending large amounts of money to persons or financial institutions in foreign countries.
 - Expressing a duty to engage in violence against DOD or the United States in support of an international terrorist cause.
 - Purchasing bomb-making materials.
 - Obtaining information about the construction and use of explosive devices or statements about acquiring materials to make a bomb.
 - Expressing support for persons or organizations that promote or threaten the unlawful use of force or violence.
 - Advocating loyalty to a foreign interest over loyalty to the United States.
 - Financial contribution to a foreign charity or other foreign cause linked to support to an international terrorist organization.
 - Evidence of terrorist training or attendance at terrorist training facilities.
 - Repeated viewing of Internet Web sites, without official sanction, that promote or support international terrorist themes.
 - Posting comments or exchanging information, without official sanction, at Internet chat rooms, message boards, or blogs that promote the use of force directed against the United States.
 - Joking or bragging about working for a foreign intelligence service or associating with international terrorist activities.
-

Table 3–3
Indicators of extremist activity that may pose a threat to DOD or disrupt U.S. military operations

- Receiving financial assistance from a person who advocates the use of violence to undermine or disrupt U.S. military operations or foreign policy.
 - Soliciting advice, encouragement, finances, training, or other resources from a person who advocates the use of unlawful violence to undermine or disrupt U.S. military operations or foreign policy.
 - Making a financial contribution to a foreign charity, an organization, or a cause that advocates the use of unlawful violence to undermine or disrupt U.S. military operations or foreign policy.
 - Expressing a political, religious, or ideological obligation to engage in unlawful violence directed against U.S. military operations or foreign policy.
 - Expressing support for foreign persons or organizations that promote or threaten the use of unlawful force or violence to achieve political, ideological, or religious objectives.
 - Participation in political demonstrations that promote or threaten the use of unlawful violence directed against the Army, DOD, or the United States based on political, ideological, or religious tenets, principals, or beliefs.
-

Chapter 4

Reporting Procedures

4-1. Individual response

Persons who know about a threat-related reportable incident or are involved in a CI-reportable situation, should do the following:

- a.* Remain calm.
- b.* If the incident involves a possible approach by foreign intelligence, remain noncommittal, neither refusing nor agreeing to cooperate.
- c.* Do not, under any circumstances, conduct your own investigation or attempt to follow the other persons involved.
- d.* Make note of the date, time, and place of the incident. Report the following information to the supporting CI office, if known or observed:
 - (1) The physical description or identity of the person making the approach.
 - (2) The license number and description of any vehicle involved.
 - (3) Names of any witnesses or others who know about it.
 - (4) Details of the incident.
- e.* Limit knowledge of a threat-related incident to persons who have an absolute need to know as detailed in paragraph 4-2.

4-2. Reporting the incident

- a.* Do not report threat-related incidents, behavioral indicators, or other matters of CI interest through serious incident report channels, security channels, inspector general channels, or in any other manner except as specified in this paragraph and paragraph 4-3.
- b.* DA personnel will report those threat-related incidents specified in paragraph 3-1 to the supporting CI office within 24 hours after learning of the incident.
- c.* DA personnel should report the behavioral indicators in tables 3-1, 3-2, and 3-3 and the other matters of CI interest in paragraph 3-3 to the supporting CI office as soon as possible after becoming aware of the information.
- d.* If a CI agent is not available or a report cannot be made directly to a CI office—
 - (1) Contact your security manager or commander, explaining that you need to report a CI incident. Security managers or commanders will refer reports as securely and expeditiously as possible, but in all cases within 24 hours of being informed of the incident, to the nearest CI office or to a CI agent organic to the unit, or
 - (2) Call the 1-800 CALL SPY (1-800-225-5779) Hotline if you are located in CONUS, or
 - (3) Use the online CI incident reporting link on Army Knowledge Online or Army Knowledge Online-SIPRNET.
- e.* When assigned or traveling outside the United States 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 office of the Naval Criminal Investigative Service, Air Force Office of Special Investigations, other U.S. military intelligence or security office, Defense Attaché Office, or U.S. Embassy or Consulate Security Office. If the matter is not urgent, report to your supporting CI office upon completion of travel.
- f.* If it is not possible to contact a CI office when deployed, follow theater-approved policy and procedures to securely and quickly report a threat-related incident.
- g.* If another person seeking to report a threat-related incident or CI matter contacts you, assist the person in contacting the supporting CI office or a CI agent organic to the unit. Do not attempt to gather and report the information yourself. The CI agent will require direct access to the person who has firsthand knowledge of the incident. Do not share knowledge of the CI incident with unauthorized third parties.

4-3. Additional reporting requirements

Incidents or behaviors that are otherwise reportable to the supporting CI office must also be reported in accordance with the cited policy, as follows:

- a.* The SAP and SMU personnel will also report CI matters to their program security officer in accordance with AR 380-381.
- b.* Known or suspected automated information system intrusions will also be reported as instructed in AR 25-2.
- c.* Known or suspected incidents of international terrorism or sabotage will be reported as serious incident reports as required by AR 190-45 and AR 525-13.
- d.* Unauthorized absences as defined in paragraph 3-3*a* will be reported in accordance with AR 630-10.
- e.* Any DA personnel exhibiting behaviors that indicate potential association with extremist activities that are directed against the Army, DOD, or the United States are reportable to the commander of the unit to which the person is assigned under the provisions of AR 600-20.
- f.* All DA personnel with a security clearance are required to report to their security office all personal foreign travel in advance of the travel and must undergo a foreign travel briefing in accordance with AR 380-67.

g. Loss or compromise of classified information, including classified information that appears in the media, must be reported immediately to the commander or security manager in accordance with AR 380–5.

h. Personnel in sensitive positions will inform their security managers in advance of any planned contact with foreign diplomatic personnel or visits to foreign diplomatic establishments.

i. Upon receipt of CIR involving foreign government representatives to the Department of the Army, including foreign liaison and exchange personnel, the ACICA will notify the Office of the Deputy Chief of Staff, G–2 (DAMI–CDS) (Foreign Disclosure Office) in accordance with the provisions of AR 380–10.

4–4. Fabricated reporting

Persons who report threat-related incidents, behavioral indicators, or CI matters which are intentionally false or fabricated may be subject to disciplinary or administrative action. (See UCMJ, Art. 107).

4–5. Obstruction of reporting

Supervisors, commanders, or security managers will not obstruct or impede any DA person from reporting a threat-related incident, behavioral indicator, or other CI matter. Except as indicated in paragraph 4–3, they will not attempt to adjudicate or handle the matter outside of CI channels.

Chapter 5

Counterintelligence Unit Reporting Policy and Procedures

5–1. Receipt of threat reports from DA personnel

Upon receipt of threat reports, the CI agents will—

a. As authorized by standing investigative authority in AR 381–20, interview the original source of a reported threat incident, behavioral indicator, or other CI matter to gather information on the facts and circumstances of the incident and the identities of all persons involved. Submit a formal CIR using the format specified in appendix B with details of the incident as reported by the source or sources. The CIRs will be classified at the CONFIDENTIAL level, at a minimum.

b. Remind reporting individuals that they are not to reveal the existence or the nature of the incident or situation to anyone else absent specific instructions from a CI agent.

c. Submit a CIR using secure communications within 72 hours after the interview of the person who reported or has knowledge of the incident. This report will be sent to the ACICA with concurrent copies to the appropriate ATCICA or Task Force Counterintelligence Coordinating Authority (TFCICA) and chain of command.

5–2. Other considerations

a. If the CI agent cannot meet the 72 hour reporting requirement due to transportation problems in a combat environment, inclement weather, lack of ability to communicate securely, or inability to locate or interview persons with firsthand knowledge of the incident, the agent will immediately notify the ACICA, or the appropriate ATCICA or TFCICA of whatever information is known about the incident and state why a report cannot be rendered within 72 hours. The CI agent may request that the reporting requirement be extended to a mutually agreed date.

b. If the CI agent is in doubt about whether the incident should be reported, the CIR will be submitted to the ACICA for a determination.

c. After submitting a CIR, CI agents will not take further action until a determination is made by the appropriate CI coordinating authority (as defined in AR 381–20) as to whether the incident merits a CI investigation.

Chapter 6

Assessment of the Threat Awareness and Reporting Program

6–1. Purpose

Using data furnished by CI units and collated by the appropriate ATCICA or TFCICA, the Director, Army G–2X will maintain statistical data on the TARP for use by DCS, G–2 to monitor and evaluate the effectiveness of the Army CI program, for use in program management and resource justifications, and to assess Army CI capabilities. The Army G–2X may also furnish this data to the ACIC for use in assessments of the CI program.

6–2. Counterintelligence unit responsibility

Counterintelligence units will produce a quarterly report on the CI unit's threat awareness program. The quarterly report will account for CI support conducted during the previous quarter and will be furnished to the appropriate ATCICA or TFCICA. At a minimum, this report will include the following:

- a.* A list of those supported units and organizations to which threat-awareness training was presented; the dates of training; the actual or estimated number of attendees at each; and the place where training was conducted.
- b.* The number of CIR which resulted from threat-awareness briefings.
- c.* A description of any significant reporting resulting from threat-awareness training.
- d.* A description of any other action taken on reports, such as, leads referred to other agencies, and so forth.
- e.* A summary of the initiatives used to promote threat awareness (newspapers, newsletters, posters, support to special activities, and so forth).
- f.* A summary of the problems or issues that are assessed as hindering the implementation of the unit Threat Awareness Program along with recommendations to improve the program.

6-3. Army service component command, Army commands, and direct reporting unit responsibility

Army service component command, Army commands, and direct reporting unit will produce a quarterly report that consolidates input from subordinate CI units as specified in paragraph 6-2. The report will be furnished to the Director, Army G-2X no later than the 20th calendar day after the beginning of the fiscal quarter. The format will correspond to paragraphs 6-2*a* to *f*.

Appendix A References

Section I Required Publications

AR 25–2

Information Assurance (Cited in para 4–3*b*.)

AR 190–45

Law Enforcement Reporting (Cited in paras 4–3*c*, glossary.)

AR 380–5

Department of the Army Information Security Program (Cited in paras 3–1*j*, 4–3*g*.)

AR 380–10

Foreign Disclosure and Contacts with Foreign Representatives (Cited in para 4–3*i*.)

AR 380–67

Personnel Security Program (Cited in para 4–3*f*.)

AR 380–381

Special Access Programs (SAPs) and Sensitive Activities (Cited in para 4–3*a*.)

AR 381–14 (C)

Technical Counterintelligence (TCI)(U) (Cited in para 3–3*j*.)

AR 381–20 (S//NF)

The Army Counterintelligence Program (U) (Cited in paras 1–9*g*, 3–3*i*, 5–1*a*, 5–2*c*, and glossary.)

AR 525–13

Antiterrorism (Cited in paras 4–3*c*, glossary.)

AR 600–20

Army Command Policy (Cited in para 4–3*e*.)

AR 630–10

Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings (Cited in paras 3–3*a*, 4–3*d*.)

Section II Related Publications

A related publication is a source of additional information. The user does not have to read it to understand the publication. DOD publications are available at <http://www.dtic.mil/whs/directives/>.

AR 1–201

Army Inspection Policy

AR 11–2

Manager's Internal Control Program

AR 380–67

The Department of the Army Personnel Security Program

AR 381–10

U.S. Army Intelligence Activities

AR 530–1

Operations Security

DOD 5240.1–R

Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons

DODD 5220.22–M

National Industrial Security Program Operating Manual

DODD 5240.02

Counterintelligence

DODI 5240.6

Counterintelligence Awareness, Briefing, and Reporting Programs

DODI 5240.16

DOD Counterintelligence Functional Services

EO 12333 (as amended 30 Jul 08)

United States Intelligence Activities

EO 12829

National Industrial Security Program

EO 12958

National Security Information

Directive–Type Memorandum (DTM) 08–007

DOD Force Protection Threat Information (Available at <http://www.dtic.mil/dtic/index.html>.)

Presidential Decision Directive/NSC 12

Security Awareness and Reporting of Foreign Contacts (Available at <http://www.dm.usda.gov/pdsd/SecurityAwarenessReportingForeignContacts.pdf>.)

18 USC

Crimes and Criminal Procedure

UCMJ, Art. 106(a)

Espionage

UCMJ, Art. 107

False statements

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

DA Form 11–2

Internal Control Evaluation Certification

DD Form 254

Department of Defense Contract Security Classification Specification

Appendix B Counterintelligence Incident Report Format

The Director, Army G-2X is the proponent for CI investigative report standards. The CIR will be properly marked with a classification on the top and bottom of each page and each paragraph will be marked using portion markings. At a minimum, the CIR will include all of the information shown below—

B-1. SUBJECT (in cases where the identity of the subject is known)

- a.* Line 1. Last name, first name, middle name.
- b.* Line 2. Grade/rank; social security number.
- c.* Line 3. Date (day, month, year) and place of birth.
- d.* Line 4. Local case control number (comprised of the field element brevity code, last two numbers of the fiscal year, and the sequence number. Example: local case control number: MID-09-001).

B-2. SUBJECT (in cases where the identity of the subject is not known or there are multiple subjects)

- a.* Line 1. City and state or country where the incident took place.
- b.* Line 2. Date of incident.
- c.* Line 3. Local case control number.

B-3. Paragraph 1. SUMMARY

Covering the basic interrogatives, summarize the CI incident in a paragraph consisting of five lines, followed by the appropriate ACOM, ASCC, or DRU; include a statement as to the possibility or probability of foreign intelligence or international terrorist involvement; and a statement about whether any military technology is involved. Fully identify all personnel, organizations, and locations in the NARRATIVE paragraph.

B-4. Paragraph 2. DATE OF INCIDENT

Day, month, and year.

B-5. Paragraph 3. LOCATION OF INCIDENT

Note the complete address where the incident took place (room, floor, building, unit, installation, street number, and name, town or city, state, and country).

B-6. Paragraph 4. PERSONS INVOLVED

Provide all known identifying data of individuals involved (last name, first name, middle name; rank; service; social security account number; date and place of birth; military occupational specialty; unit of assignment; city, state, or country; residence address; phone numbers (office, home, cell); expiration of term of service; permanent change of station date; deployment dates; security clearance; access to classified information; and access to digital media). If identifying information is not known, provide physical description (gender; race; complexion; age; height; weight; build; hair color and style; eye color and glasses; dress; and distinguishing characteristics).

- a.* SUBJECT(S).
- b.* SOURCE(S).
- c.* WITNESS(ES).
- d.* OTHERS KNOWLEDGEABLE.

B-7. PRIVACY ACT CAVEAT

Preface the NARRATIVE with a Privacy Act caveat that reflects the source's response to the Privacy Act advisory provided by the CI agent prior to the conduct of the interview. Three common Privacy Act Caveats (capitalized) are:

- a.* SOURCE HAD NO OBJECTION TO HIS OR HER IDENTITY BEING DISCLOSED.
- b.* SOURCE HAD NO OBJECTION TO HIS OR HER IDENTITY BEING RELEASED TO SUBJECT.
- c.* SOURCE REQUESTED CONFIDENTIALITY AS A CONDITION OF PROVIDING INFORMATION IN THIS REPORT.

B-8. Paragraph 5. NARRATIVE

Describe the details of the incident as related by the source, in chronological order; be concise.

B-9. Paragraph 6. ACTIONS TAKEN

Describe all actions taken by the reporting CI unit in connection with the incident reported.

B-10. Paragraph 7. AGENT'S COMMENTS

Clarify information contained in the preceding NARRATIVE paragraph, as necessary. Describe proposed courses of action along with any recommendation for disposition of the incident.

B-11. Paragraph 8. REPORT PREPARED BY

The CI agent who prepared the report, the identity of his unit, a secure phone number, a secure facsimile number, and a SIPRNET e-mail address.

B-12. Paragraph 9. EXHIBITS

List all attachments to the report and the dates on which the documents were received.

Appendix C Internal Control Evaluation Certification

C-1. Function

The function of this evaluation is to ensure effective implementation of the Army's TARP.

C-2. Purpose

The purpose of this evaluation is to provide feedback to unit commanders regarding compliance with the training and reporting procedures specified in this regulation.

C-3. Instructions

Answers must be based upon actual testing of key internal controls such as document analysis, direct observation, interviews, sampling, and simulation. Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These internal controls *must* be evaluated annually, each time a Command Inspection Program occurs, or at a minimum, once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11-2 (Internal Control Evaluation Certification).

C-4. Test questions

a. Army commanders.

- (1) Established unit procedures on threat awareness and reporting?
- (2) Included threat awareness and reporting in the organizational inspection program?
- (3) Maintained a roster of unit members trained in threat awareness and reporting?
- (4) Maintained a training calendar that includes annual training on threat awareness and reporting?
- (5) Maintained contact information for the supporting CI unit (identity of office, names of CI agents, phone numbers, and e-mail addresses)?

b. Counterintelligence unit commanders.

- (1) Established procedures for the preparation and conduct of threat awareness training?
- (2) Established a professional, relevant, and timely Threat Awareness Program as a priority for the unit's mission of developing CI leads?
- (3) Ensured that assigned CI agents responded in a timely manner to those threat incidents, behavioral indicators, and other matters of CI interest specified in chapter 3 when such matters are reported by DA personnel?
- (4) Included threat awareness and reporting in the Organizational Inspection Program?
- (5) Coordinated with other intelligence, law enforcement, and force protection agencies to acquire threat data for inclusion in threat awareness training?
- (6) Established a Covering Agent Program which includes threat-awareness training, special threat-awareness training, and debriefings?
- (7) Maintained records of units or organizations which received threat-awareness training; the number of DA personnel in each who were trained; the dates of training; the location of training; and any significant results of training?
- (8) Maintained a calendar for scheduling future training on threat awareness?
- (9) Maintained contact information on each supported organization?
- (10) Submitted a quarterly report on the unit's awareness program as required by paragraph 6-2?
- (11) Submitted CI incident reports within 72 hours after the interview of the person or persons who reported the incident?

C-5. Supersession

This is the initial checklist for the Threat Awareness and Reporting Program.

C-6. Comments

Help make this a better tool for evaluating internal controls. Submit comments to the Deputy Chief of Staff, G-2, 1000 Army Pentagon, Washington, DC 20310-1000.

Glossary

Section I Abbreviations

ACIC

Army Counterintelligence Center

ACICA

Army Counterintelligence Coordinating Authority

ACOM

Army command

AKO

Army Knowledge Online

ARNG

Army National Guard

ASCC

Army service component command

ATCICA

Army Theater Counterintelligence Coordinating Authority

CI

counterintelligence

CIR

counterintelligence incident report

CONUS

continental United States

DA

Department of the Army

DCS, G-2

Deputy Chief of Staff, G-2

DIA

Defense Intelligence Agency

DOD

Department of Defense

DRU

direct reporting unit

FIS

foreign intelligence service

HQDA

Headquarters, Department of the Army

INSCOM

U.S. Army Intelligence and Security Command

OCONUS

outside the continental United States

RDA

research, development and acquisition

SAP

Special Access Program

SCI

Sensitive compartmented information

SMU

special mission unit

TARP

Threat Awareness and Reporting Program

TFCICA

Task Force Counterintelligence Coordinating Authority

TRADOC

U.S. Army Training and Doctrine Command

UCMJ

Uniform Code of Military Justice

USC

United States Code

USAR

U.S. Army Reserve

Section II**Terms****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 (EO 12333, amended 30 July 2008).

Counterintelligence investigation

A duly authorized, systematic, detailed examination or inquiry to uncover facts to determine the truth of a matter regarding a person or other entity who is or may have engaged in espionage; to detect and identify foreign intelligence collection against the U.S. Army; to detect and identify other threats to national security; to determine the plans and intentions of any international terrorist group or other foreign adversary which presents a threat to lives, property, or security of Army forces or technology; to neutralize terrorist operations against U.S. Forces; to collect evidence for eventual prosecution for national security crimes; to determine the extent and scope of damage to national security; and to identify systemic vulnerabilities (AR 381–20).

Counterterrorism

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

Critical program information

Elements or components of a research, development, and acquisition program that, if compromised, could cause significant degradation in mission or combat effectiveness; shorten the expected combat-effective life of the system;

reduce technological advantage; significantly alter program direction; or enable a foreign adversary to defeat, counter, copy, or reverse engineer the technology or capability (AR 381–20).

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.

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).

PORTICO

A program managed by the Defense Counterintelligence and Human Intelligence Center, DIA, to provide automation support to the DOD CI community through Web-enabled software (DODI 5240.6).

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.

Sedition

An act or acts intending to cause the overthrow or destruction of the U.S. 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 the duty, necessity, desirability, or propriety of overthrowing or destroying by force or violence the U.S. Government.

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 Headquarters (AR 190–45).

Special agent, counterintelligence

Personnel holding MOS 35L, 351L, and 35E as a primary specialty, and civilian personnel in the GG–0132 career field, who have successfully completed the Counterintelligence Special Agent Course and who are authorized to be issued counterintelligence 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.

Subversion

An act or acts inciting military or civilian personnel of the DOD 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).

Suspicious activity

Any behavior that is indicative of criminal activities, intelligence gathering, or other preoperational planning related to a security threat to DOD interests (DTM 08–007). (See UCMJ, Art. 106a.)

Terrorism

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

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 possible, report it.

Section III**Special Abbreviations and Terms****Agent of a foreign power**

a. Any person, other than a U.S. citizen, who—

(1) 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 terrorist activities.

(2) 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.

(3) Indicates (by circumstances of the person's presence in the United States) that he or she may engage in such activities in the United States.

(4) Knowingly aids and abets any person in conducting such activities.

(5) Knowingly conspires with any person to engage in such activities.

b. Any person who—

(1) 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.

(2) 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.

(3) Knowingly prepares for or engages in sabotage or international terrorism for or on behalf of a foreign power.

(4) 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.

Clandestine intelligence activity

An activity conducted by or on behalf of a foreign power for intelligence purposes or for the purpose of affecting political or governmental processes if the activity is conducted in a manner designed to conceal from the U.S. Government the nature or fact of such activity or the role of such foreign power; also, any activity conducted in support of such activity.

DA personnel

Members of the active Army, the ARNG/Army National Guard of the United States, the USAR, DA civilian personnel, contractor personnel, and foreign nationals employed by the DA.

Extremist activity

As used in this regulation, an activity that involves the use of unlawful violence or the threat of unlawful violence directed against the Army, DOD, or the United States based on political, ideological, or religious tenets, principals, or beliefs.

False flag approach

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

Insider threat

A person with placement and access who intentionally causes loss or degradation of resources or capabilities or compromises the ability of an organization to accomplish its mission through espionage, providing support to international terrorism, or the unauthorized release or disclosure of information about the plans and intentions of U.S. military forces (AR 381–20).

Supporting counterintelligence office

A CI office assigned responsibility for supporting a command, facility, program, installation, or geographic area.

Threat

The activities of foreign intelligence services, foreign adversaries, international terrorist organizations, or extremists that may pose a danger to the Army, DOD, or the United States; any person with access to Soldiers, DOD installations, and facilities who may be positioned to compromise the ability of a unit to accomplish its mission where there is evidence to indicate that he may be acting on behalf of or in support of foreign intelligence, foreign adversaries, international terrorists, or extremist causes (insider threat).

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

Requests for information from a person which may range from direct inquiries by phone, e-mail, fax, or letter in which the recipient is asked to provide seemingly innocuous data. Typical requests include solicitation of research papers, requests for additional information after a public presentation, suggestions for mutual research, requests for survey participation, and so forth; correspondence where 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.

UNCLASSIFIED

PIN 004111-000