Army Regulation 381–12

Military Intelligence

Threat Awareness and Reporting Program

Headquarters
Department of the Army
Washington, DC
1 June 2016

UNCLASSIFIED

SUMMARY of CHANGE

AR 381–12
Threat Awareness and Reporting Program

This major revision, dated 1 June 2016---

- Establishes the iSALUTE online reporting portal for submission of reportable counterintelligence incidents (paras 1-5*b*(3), 1-5*d*(6), 1-6*i*, 1-10*j*, 2-5*p*, and 4-2*d*(5)).

- Establishes policy for development of the Threat Awareness and Reporting Program stand alone briefing tool and the computer Web-based alternative training modules (paras 1-5*b*(4), 1-11*d*, 2-4*c*, and 2-4*d*).

- Establishes the Threat Awareness and Reporting Program's train the trainer program (paras 1-5*b*(7), 1-5*c*(3), 1-7*c*, 1-11*c*, 2-4*b*, 2-4*g*, 2-7*e*, and 2-9).

- Mandates that only Deputy Chief of Staff, G-2-approved Threat Awareness and Reporting Program media will be used to conduct training (paras 1-5*c*(2), 1-7*b*, 1-10*c*, and 2-4*c*).

- Requires the Commander, U.S. Army Intelligence and Security Command, to assist combatant commands, defense agencies, and Department of Defense field activities, for which Army is the lead agency in developing counterintelligence awareness programs, to meet their requirement to comply with Department of Defense Directive 5240.06 (para 1-5*c*(11)).

- Requires counterintelligence incident reports to be populated in the Army Counterintelligence Operations Portal, when available (paras 1-5*c*(13), 1-5*d*(3), 1-11*g*, and 5-1*c*).

- Adds responsibility for principal officials, Headquarters, Department of the Army, to ensure their personnel receive Threat Awareness and Reporting Program training and report incidents (para 1-6).

- Makes live Threat Awareness and Reporting Program training mandatory, except in exceptional circumstances (paras 1-6*b*, 1-6*m*, 1-7*a*, 1-10*c*, 1-10*k*, 2-3*a*, 2-4*a*, and 2-4*i*).

- Requires principal officials, Headquarters, Department of the Army and commanders of Army commands, Army service component commands, and direct reporting units to develop a process to track Threat Awareness and Reporting Program training (para 1-6*g*).

- Makes the training and reporting requirements of this regulation applicable to all Army contractors if included in the applicable contract, not just those with security clearances (paras 1-6*l* and 1-10*k*).

- Authorizes the National Guard Bureau and the U.S. Army Reserve Command to use properly trained non-counterintelligence agents to present Threat Awareness and Reporting Program briefings (para 1-7*c*).

- Requires counterintelligence units to designate a senior person to oversee the unit's implementation of the Threat Awareness and Reporting Program (para 1-11*a*).

- Adds a table with reportable indicators of potential exploitation of Department of Defense information systems from hostile external actors or insider threats (table 3-4).

Headquarters
Department of the Army
Washington, DC
1 June 2016

*Army Regulation 381–12

Effective 1 July 2016

Military Intelligence

Threat Awareness and Reporting Program

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the Secretary of the Army

History. This publication is a major revision.

Summary. This regulation implements Department of Defense Directive 5240.06. It provides policy and responsibilities for threat awareness and education and establishes a requirement for Department of Army 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 Department of the Army Civilian personnel, Army contractors as incorporated by the terms of the contract, and foreign nationals employed by the Army. The applicability of this regulation to local foreign 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.

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 internal controls that must be evaluated (see app B).

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)

*This regulation supersedes AR 381–12, dated 4 October 2010.

UNCLASSIFIED

Contents—Continued

Contents—Continued

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
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Responsibilities
Responsibilities are listed in section II of chapter 1.

Section II
Responsibilities

1–5. Deputy Chief of Staff, G–2
a. The DCS, G–2 will—

(1) As the senior intelligence officer of the Army, exercise Army staff responsibility for policy and procedures related to threat awareness and reporting.

(2) 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.

(3) Oversee the implementation of the TARP and ensure its effectiveness as an element of the Army's overall CI effort.

(4) Establish policy and guidelines for the processing, investigation, and disposition of matters and incidents reported by Army personnel under this regulation, as appropriate.

(5) Ensure that the Army leadership is aware of significant threat and other CI related incidents.

b. The Director, Army G–2X, on behalf of the DCS, G–2, will——

(1) Ensure that TARP is implemented as a priority program for the development of CI leads.

(2) Consolidate TARP statistical reporting across the Army as specified in chapter 6 and conduct an assessment of the effectiveness of program at least annually.

(3) Manage the iSALUTE online CI reporting portal or any successor system, and develop policy and procedures for its use.

(4) Oversee the development of TARP training modules in coordination with the U.S. Army Intelligence and Security Command (INSCOM), set standards for content, and serve as the approval authority for the final products. Training modules are the stand alone briefing tool (SBT) and the computer Web-based alternative training (CBT), or any modules that may be developed as a follow on to these tools.

(5) Ensure that the TARP SBT includes modules that relate to large groups of specialized audiences, including but not necessarily limited to, audiences consisting largely of Army contractors and audiences that may be made up exclusively of Government civilian personnel.

(6) Ensure that SBT modules are modified as needed to ensure that the message remains timely, relevant, and fresh.

(7) Oversee implementation of the TARP train the trainer (T3) program by Commander, INSCOM.

c. Commander, INSCOM will——

(1) In coordination with the DCS, G–2, develop TARP training modules that meet the standards of this regulation; that are current, relevant, and timely; and that meet other standards that may be set by the DCS, G–2.

(2) Implement TARP training in support of Army units worldwide through subordinate commands. Ensure that only the DCS, G–2 approved TARP media are used to conduct training.

(3) Develop, implement, and resource the T3 program and ensure that TARP training is presented in a professional and knowledgeable manner.

(4) 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.

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

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

(7) Assist supported units in developing programs to publicize the importance of threat reporting.

(8) As appropriate, conduct follow-on CI investigations of CI incidents as specified in Army Regulation (AR) 381–20.

(9) Through the Army Counterintelligence Center (ACIC), use data from closed CI investigations and assessments of trends in foreign intelligence and international terrorism for developing current, relevant, and timely revisions to the TARP SBT.

(10) Produce an annual report on the foreign intelligence and international terrorist threat to the Army.

(11) Assist those combatant commands, defense agencies, and DOD field activities for which Army has lead for CI support, in the development of CI awareness training to meet their requirement for compliance with DOD Directive (DODD) 5240.06. The TARP training standards of this regulation, when the training is conducted by Army CI agents, are sufficient for compliance with DODD 5240.06.

(12) Through commanders, 902d Military Intelligence (MI) Group (Continental United States (CONUS)), 66th MI Brigade (Europe), and 501st MI Battalion (Korea), monitor calls received from the CALL SPY Hotlines specified in paragraph 4–2*d* and assign investigative responsibility for leads developed, as appropriate.

(13) Ensure that CI investigative elements use the Army CI Operations Portal (ACOP) or any successor system to populate and record CI incident reports (CIRs).

d. The Director, Army Counterintelligence Coordinating Authority (ACICA), INSCOM G–2X, will—

(1) Coordinate, deconflict, and centrally manage TARP reporting across the Army and serve as the focal point for the assessment of CIRs as a basis for CI investigations.

(2) Ensure that CI reporting from the National Guard Bureau or the U.S. Army Reserve (USAR) for which Army does not have investigative jurisdiction as specified in AR 381–20 is referred to the Federal Bureau of Investigation (FBI) or other appropriate agency.

(3) Manage the operation of ACOP.

(4) In coordination with the ACIC, ensure that data from closed CI investigations is shared with the TARP Training Team for use in developing current, relevant, and timely revisions to the TARP SBT.

(5) Serve as the approval authority for the release of information from closed CI investigations for use in developing revisions to the SBT.

(6) Monitor CI reporting from iSALUTE and ensure that leads are assigned to the appropriate CI investigating element for follow-up or referred to another agency for action, as appropriate.

e. Commander, 650th MI Group will——

(1) Implement the threat awareness program in support of organizations, personnel, and installations of the North Atlantic Treaty Organization (NATO), Allied Command Operations, and Allied Command Transformation.

(2) Ensure that the content of threat awareness training is tailored to the mission, geography, and degree of potential hostile intelligence or international terrorist threat to NATO.

(3) Ensure that threat awareness training is 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 events.

(4) Through the Allied CI Coordinating Authority (ACCA), provide oversight of the threat awareness and reporting program in support of NATO.

1–6. Principal officials, Headquarters, Department of the Army and commanders, Army commands, Army service component commands, and direct reporting units

Principal officials, Headquarters, Department of the Army and commanders of ACOMs, ASCCs, and DRUs will—

a. Designate a senior person, preferably on the G–2 staff, to oversee the command's implementation of the TARP program and to perform the other duties outlined in this paragraph (applicable to commanders of ASCCs).

b. Ensure that all DA personnel under their cognizance attend live CI awareness training annually, conducted either by CI agents representing the supporting CI unit or by organic CI agents, if available.

c. Provide command emphasis on the importance of threat reporting.

d. Ensure that DA personnel are knowledgeable of those reportable threat-related incidents and behavioral indicators in chapter 3 and know how to report incidents as specified in chapter 4.

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

f. 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.

g. Develop a process to track TARP training on those installations for which they have cognizance to ensure that all personnel receive live annual TARP training.

h. Include the training and reporting requirements of this regulation in command inspection programs.

i. Post a link to the iSALUTE online CI reporting portal on all Army public domain Web sites for which they have cognizance.

j. For ASCCs with an INSCOM theater intelligence group or brigade OPCON to them, oversee compliance with the CI aspects of this regulation.

k. Ensure that online training using the CBT is used only in the circumstances outlined in paragraph 2–4*i*. The first O–6 or civilian equivalent in the chain of command must approve any organization-wide training that is conducted using the CBT under circumstances that are not outlined in paragraph 2–4*i*.

l. Ensure that the threat awareness and reporting requirements of this regulation are incorporated into Army contracts via the statement of work or on DD Form 254 (Department of Defense Contract Security Classification Specification) for classified contracts. Coordinate with the appropriate contracting officer if the contracts must be modified to ensure compliance.

m. Subject to the incorporation of these requirements into the contract, ensure that contractors over whom they have cognizance attend live TARP training at least annually and 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 FBI, or the Defense Security Service.

1–7. Chief, National Guard Bureau and Chief, Army Reserve

CNGB and CAR will—

a. Ensure that live threat awareness training is provided to USAR and Army National Guard (ARNG) personnel at least annually, as required by this regulation.

b. Ensure that threat awareness training is presented using the G–2 approved training media and delivered by personnel who have completed the TARP briefers training.

c. Because of the geographic dispersion of ARNG and USAR units, the National Guard Bureau and the USAR Command are authorized to use non-CI agents of other intelligence military occupational specialties (MOSs) to present TARP briefings. These personnel must successfully complete the TARP briefers training conducted by the 902d MI Group. Non-CI agents completing the TARP briefers training may present TARP briefings, but are not authorized to train other National Guard and USAR personnel to present briefings. See paragraph 1–11*c* for requesting T3 and TARP briefers training.

d. Members of Reserve and National Guard units will refer those matters or incidents defined in chapter 3 and in tables 3–1 to 3–4 to nearest office of the 902d MI Group or to the ACICA.

e. Ensure that special threat awareness training as defined in paragraphs 2–6 and 2–7 is conducted, when applicable.

1–8. Commanders, U.S. Army Forces Command and U.S. Army Special Operations Command

Commanders, FORSCOM and USASOC will identify CI agents for attendance at the TARP T3 program conducted by the 902d MI Group and, once certified, use them to present TARP training to FORSCOM and USASOC units, respectively. Submit TARP statistical reports quarterly as specified in paragraph 6–3.

1–9. 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 TARP is incorporated into all Army leadership courses under TRADOC cognizance to familiarize students with command and individual responsibilities and the role of the supporting CI unit.

1–10. All Army commanders

Army commanders at all levels will—

a. Place command emphasis on the importance of prompt threat reporting, ensuring 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. Incorporate threat awareness training into unit training schedules and ensure that all DA personnel and Army contractors (if compliant with the terms of the contract), receive annual threat awareness training conducted by a CI agent or other trainer as specified in paragraph 2–4.

c. Ensure that TARP training is conducted in a live environment and that online training using the CBT is used only

when the conditions in paragraph 2–4*i* apply. The first O–6 in the chain of command must approve any organization-wide training that is conducted using the CBT under circumstances that are not outlined in paragraph 2–4*i*.

d. Report incidents directly to the supporting CI office, whenever possible; use the online reporting portal; or use the CALL SPY Hotline as specified in paragraph 4–2. Reporting directly to the supporting CI office preserves the integrity of any ensuing investigation.

e. Not discuss the details of any incident that they have reported to anyone else unless authorized by the CI agent. This requirement does not preclude Army personnel from reporting the details of any intelligence oversight issue that is reportable to the Inspector General as required by AR 381–10. Any command briefings or notifications that may be required will be accomplished by the CI agent.

f. 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.

g. Inspect compliance with the threat awareness and reporting requirements of this regulation in unit command inspection programs in accordance with appendix B.

h. Administer judicial or administrative action, as appropriate, pursuant to applicable law or policy, when personnel fail to report threats as described in paragraph 3–1.

i. 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).

j. Post a link to the iSALUTE online CI reporting portal on all Army public domain Web sites for which they have cognizance.

k. Ensure that the threat awareness and reporting requirements of this regulation are incorporated into Army contracts via the statement of work or on the DD Form 254 for classified contracts. Commanders should coordinate with the appropriate contracting officer if the contract must be modified to ensure compliance.

l. Subject to the incorporation of these requirements into the appropriate contract, ensure that contractors over whom they have cognizance attend live TARP training at least annually and that they 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 FBI, or the Defense Security Service.

1–11. Unit commanders with counterintelligence personnel assigned or attached

Unit commanders with CI personnel assigned or attached will—

a. Designate a senior person to oversee the unit's implementation of TARP and to ensure that TARP training is presented in a professional and knowledgeable manner.

b. Support all Army commanders in the unit's geographic area of responsibility with TARP training.

c. Ensure that all CI agents conducting TARP training have successfully completed the T3 program administered by the 902d MI Group and are certified to conduct training. The training team may be contacted at usarmy.meade.902-mi-grp.mbx.902d-mi-gp-tarp@mail.mil.

d. Ensure that only the DCS, G–2 approved standardized TARP training module is used in TARP presentations.

e. 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.

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

g. Submit CIR using ACOP (when it becomes operational) within 72 hours of receipt of a report from a source or within 72 hours of the unit acquiring information about a reportable event.

h. Submit CIR simultaneously to the ACICA, the CONUS CI Coordinating Authority (CICA) or the appropriate Army Theater CI Coordinating Authority (ATCICA), and the appropriate CI operational chain of command.

i. Units deployed in support of combatant commanders will submit CIR directly to the ACICA with information copies to the appropriate task force CI Coordinating Authority (TFCICA). As specified in DODD 5240.02, Army CI units that are deployed in a combat theater under operational control of a combatant commander will conduct CI investigations and related activities under the authority, direction, and control of the Secretary of the Army.

j. 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.

k. 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.

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

m. 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.

n. When the CI unit does not have the resources to support all units in its area of responsibility (AOR) with live training, the CI commander may prioritize this support, so that organizations with the most sensitive missions or those that are deploying have the highest priority.

1–12. Contracting officers

The requirements of this regulation will be incorporated into contracts and made applicable to those contracts in accordance with DOD Directive 5240.06.

Chapter 2
Threat Awareness and Education

Section I
General

2–1. Army as a target

a. The Army is a prime target for exploitation by foreign intelligence and international terrorist organizations. The Army faces the threat of espionage, sabotage, subversion, and international terrorism from within the United States and outside the continental United States (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 Department of the Army 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 warfighting mission and in protecting the lives of Soldiers.

2–3. Threat awareness policy

a. All DA personnel will receive TARP training within 30 days of assignment or employment to an organization and will undergo live environment TARP training at least annually. Live training is mandatory unless the conditions in paragraph 2–4*i* apply.

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.

d. DA personnel who have completed annual live training are not required to complete online training.

Section II
Threat Awareness Training

2–4. Conduct of threat awareness training

a. Annual threat awareness training conducted by a CI agent making the presentation to a live audience is mandatory for all DA personnel unless the conditions in paragraph 2–4*i* apply. Live training allows the trainer to tailor the SBT 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.

b. Threat awareness training will be presented only by CI agents who have successfully completed the TARP T3 program and are certified to conduct the training. Non-CI agents assigned to National Guard and USAR units may conduct training as specified in paragraph 1–7. The 902d MI Group T3 training team may be contacted at usarmy.meade.902-mi-grp.mbx.902d-mi-gp-tarp@mail.mil.

c. Only the DCS, G–2 approved training media (the SBT) is authorized to satisfy TARP training requirements.

d. CI units will use the SBT to tailor TARP training to the audience and geographic area.

e. 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.

f. Contractors employed by units with a CI mission who have successfully completed the T3 program may present TARP training if within the terms and scope of their contract.

g. Local national investigators employed by OCONUS units with a CI mission who have successfully completed the T3 program may present TARP training to local national audiences.

h. ARNG and USAR units may use non-CI agents to present training as specified in paragraph 1–7*c*.

i. When live training is not possible, such as in deployed theaters of operation, units in remote locations without access to CI support, or when the supporting CI unit does not have the resources to conduct the training, units will

complete the CBT that is available on the Army Learning Management System (ALMS) Web site at https://www.lms.army.mil. This is the only authorized alternative method for TARP training.

j. Any organization-wide training that is not conducted live in which the conditions in paragraph 2–4*i* do not apply must be approved by the first O–6, or civilian equivalent, in the chain of command. Prior to pursuing this course of action, the unit will coordinate with the supporting CI office to determine whether a CI agent is available to conduct live training.

2–5. Content of threat awareness training

The SBT and CBT will include the following elements, at a minimum:

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 that highlight these methods.

c. The methods used by international terrorists to target Army personnel and installations and the vulnerabilities that terrorists exploit.

d. The fact that an insider threat may exploit knowledge of a unit's plans and intentions to provide operational information to the enemy or pose a potential terrorist associated threat.

e. The types of situations and indicators of both espionage and international terrorism that should be reported.

f. The provisions of the Uniform Code of Military Justice (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. The damage that espionage and the terrorist insider have caused to U.S. national security using recent examples.

h. 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.

i. 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.

j. Cautions against posting information on social networking sites about a person's official duties, military plans and intentions, or any other information which may be exploited by a foreign intelligence service or international terrorist organization.

k. Unsolicited correspondence and how it is used by foreign intelligence organizations.

l. Foreign intelligence interest in critical military technology and the methods of targeting Army personnel working in research, development, and acquisition (RDA) programs and facilities.

m. How to respond to and report threat-related incidents.

n. Cyber threats to DOD information systems and the means to prevent, reduce, or minimize them.

o. Media leaks of classified information and the observable actions of leakers that should be reported to CI.

p. The CALL SPY Hotlines in the United States, Europe, and Korea, as appropriate, and the iSALUTE online reporting system linked on all Army Web sites.

q. 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.

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. 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 especially vulnerable personnel scheduled to travel as indicated in paragraph 2–6*a* will coordinate with the servicing CI unit to arrange pre-travel threat briefings and debriefings. The following are examples of personnel who 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) or the Department of State. 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 foreign countries, who have foreign business connections or financial interests, 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 (SMUs).

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 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.

e. The CI agent need not be T3 certified to conduct these briefings. The SBT should not be used.

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 newspapers, 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 O–5 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. CI agents need not be T3 certified to conduct supplemental training and use of the SBT is optional. Situations that may indicate the need for additional threat awareness training include, but are not limited to the following:

a. Mass unit in-processing or out-processing.

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 in this chapter in accordance with the reporting instructions in chapter 4. Personnel subject to the UCMJ who fail to comply with the requirement to report the incidents in *a* through *r*, of this paragraph, below, 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 paragraph 3–1 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 known or suspected incident of unauthorized disclosure of classified information. Includes any DA person who has deliberately leaked classified or sensitive information to any unauthorized person or to any person not authorized to have knowledge of it, including the media; who has attempted to disclose information; who has voiced the intent to disclose information; or who has posted classified or sensitive information to any unauthorized Web site. (These incidents will also be reported as compromises of classified information as required by AR 380–5.)

i. 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.

j. 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.

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 or attempt or threaten to defect. The return to military control of U.S. military and civilian defectors.

3–2. Behavioral threat indicators

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; those associated with extremist activity that may pose a threat to the Army or DOD; or any potential exploitation of DOD information systems from external actors or insider threats. These indicators are described in tables 3–1 to 3–4. 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.

Table 3–1
Indicators of espionage

Behaviors	Indicators
Foreign influence or connections	• 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 in a foreign country, excluding the ownership of mutual funds or like investments in foreign companies. • 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 purposes	• Discussing classified information in unauthorized locations or over a non-secure communications device. • 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	• Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities. • Attempts to obtain classified or sensitive data not related to a work requirement or 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.

Table 3–1
Indicators of espionage—Continued

Behaviors	Indicators
Financial matters*	• 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*	• 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	• 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	• 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.

Legend for Table 3-1:
* Failure to report these matters may not form the sole basis for disciplinary action.

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

• Advocating support for international terrorist organizations or objectives.

• Expressing a hatred of American society, culture, government, or principles of the U.S. Constitution that implies support for or connection to an international terrorist organization.

• 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.

• Procuring supplies and equipment, purchasing bomb making materials, or obtaining information about the construction and use of explosive devices.

• 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 or other material support to a foreign charity or other foreign cause linked to support to an international terrorist organization.

• Evidence of training with or attendance at training facilities of international terrorist organizations.

• Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.

• Familial ties or other close associations to known or suspected members of an international terrorist organization or those supporting terrorism.

• Repeated viewing, without official sanction, of Internet Web sites 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.

Legend for Table 3-2:
* Failure to report these matters may not form the sole basis for disciplinary action.

Table 3–3
Indicators of extremist activity that may pose a threat to Department of Defense 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, principles, or beliefs.

Table 3–4
Indicators of potential exploitation of Department of Defense information systems from hostile external actors or insider threats

• Excessive probing or scanning from either an internal or external source.

• Tampering with or introducing unauthorized elements (data, software, or hardware) into information systems.

• Hacking or password cracking activities.*

• Unauthorized network access or unexplained user account.*

• Social engineering, electronic elicitation, e-mail spoofing, or spear phishing.*

• Use of DOD account credentials by unauthorized parties.

• Downloading, attempting to download, or installing non-approved computer applications.

• Key logging.

• Rootkits, remote access tools, and other “backdoors.”

• Unauthorized account privilege escalation.

• Account masquerading (when a user changes his or her own credentials to look like another user’s credentials).

• Unexplained storage of encrypted data.*

• Encryption or steganography data propagation internally.

• Unauthorized use of universal serial bus, removable media, or other transfer devices.

• Denial of service attacks or suspicious network communication failures.*

• Exfiltration of data to unauthorized domains or cross domain violations.*

• Unauthorized e-mail traffic to foreign destinations.

• Unauthorized downloads or uploads of sensitive data.

• Malicious codes or blended threats such as viruses, worms, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.*

• Data or software deletion.

• Log manipulation.

• Unauthorized use of intrusion detection systems.

Legend for Table 3-4:

* Failure to report these matters may not form the sole basis for disciplinary action.

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, SAP, 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. (Disclosure of protected health information will be consistent with DoD 6025.18–R).

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 or by any unauthorized entity.

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 (USSS) (see AR 381–20). These matters should be reported immediately to the USSS.

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.)

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

(1) Requests to obtain classified or unclassified official Government information.

(2) A query about their official duties, where they are stationed or where they work, 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, especially if in a foreign country other than the one in which the DA person is stationed.

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 to 3–4.

m. Incidents in which DA personnel deliberately violate policy or procedures in the processing of classified information using information systems or digital media.

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 an 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 the incident.

(4) If providing the report in person, include the 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.

f. When using the CALL SPY Hotline or reporting the incident online, provide only that information which the CI agent will need in order to contact you. Do not provide details of the incident or matter over the telephone or online.

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, command 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 to 3–4 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 the United States or in one of the 21 countries where the system may be used; or,

(3) Call the European CALL SPY Hotline at DSN 537–2176 or COM 49611–143–537–2176; or,

(4) Call the Korean CALL SPY Hotline at DSN 723–3299 or COM 82–05033–723–3299; or,

(5) Use the iSALUTE online CI incident reporting link on all Army public Web sites (https://www.inscom.army.mil/isalute/).

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 may be a predictor of workplace violence or may 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 DA, including foreign liaison and exchange personnel, the ACICA will notify the Office of the DCS, G–2 (DAMI–CDS) (Foreign Disclosure Office) in accordance with the provisions of AR 380–10.

j. Any questionable or adverse suitability information or any information that may reflect unfavorably on or place into question an individual's eligibility to possess a security clearance or perform sensitive duties will be reported immediately to the person's commander or security manager in accordance with AR 380–67. CI agents will advise security managers of the requirement to enter such information into the Joint Personnel Adjudication System (JPAS).

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 of administrative action. (See UCMJ, Article 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 Department of the Army 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 by the ACICA, including 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. This requirement does not preclude Army personnel from reporting the details of an intelligence oversight issue that is reportable to the Inspector General as required by AR 381–10

c. Submit a CIR using ACOP, any successor system, or another secure method of transmission, 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, CONUS CICA, or 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 explain 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.c.

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 quarterly reports on the unit's TARP program. The report is due to the Army G–2X not later than the 20th of the month following the end of each fiscal quarter. The report may be furnished to the appropriate ATCICA or CONUS CICA for consolidation at the theater level, if that is the preferred method. 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, and the actual or estimated number of attendees at each.

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.

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 TARP along with recommendations for improvement.

6–3. Reporting from commands without U.S. Army Intelligence and Security Command counterintelligence units
Commanders, AMC, TRADOC, FORSCOM, and USASOC and CNGB and USAR will produce a quarterly report that consolidates input from subordinate commands, as appropriate, to the Army G–2X using the timeline in paragraph 6–2. This report will include a list of those supported units to which TARP training was presented, the dates of training, and the estimated number of attendees at each.

Appendix A
References

Section I
Required Publications

AR 25–2
Information Assurance (Cited in para 4–3b.)

AR 190–45
Law Enforcement Reporting (Cited in para 4–3c.)

AR 380–5
Department of the Army Information Security Program (Cited in para 3–1h.)

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives (Cited in para 4–3i.)

AR 380–67
Personnel Security Program (Cited in para 4–3f.)

AR 380–381
Special Access Programs (SAPs) and Sensitive Activities (Cited in para 4–3a.)

AR 381–14
Technical Surveillance Countermeasures (U) (Cited in para 3–3j.)

AR 381–20
The Army Counterintelligence Program (Cited in para 1–5c(8).)

AR 525–13
Antiterrorism (Cited in para 4–3c.)

AR 600–20
Army Command Policy (Cited in para 4–3e.)

AR 630–10
Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings (Cited in para 3–3a.)

DODD 5240.06
Counterintelligence Awareness and Reporting (Cited in para 1–5c(11).)

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. Unless otherwise stated, Army publications are available at http://www.apd.army.mil/. DOD issuances are available at http://www.dtic.mil/whs/directives/index.html.

AR 1–201
Army Inspection Policy

AR 11–2
Managers' Internal Control Program

AR 25–30
Army Publishing Program

AR 381–10
U.S. Army Intelligence Activities

AR 530–1
Operations Security

Army Directive 2013–18
Army Insider Threat Program

DOD 5220.22–M
National Industrial Security Program Operating Manual

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

DODD 5205.16
The DOD Insider Threat Program

DODD 5240.02
Counterintelligence

DODI 5240.10
Counterintelligence in the Combatant Commands and Other DOD Components

DODI 5240.16
Counterintelligence Functional Services

DODI 5240.26
Countering Espionage, International Terrorism, and the Counterintelligence Insider Threat

DODI 5400.11
Department of Defense Privacy Program

DoD 6025.18–R
Department of Defense Health Information Privacy Regulation

Executive Order 12333 (as amended 30 Jul 08)
United States Intelligence Activities (Available at http://www.archives.gov/federal-register/executive-orders/disposition.html.)

Executive Order 12829
National Industrial Security Program (Available at http://www.archives.gov/federal-register/executive-orders/disposition.html.)

Executive Order 13587
Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Available at http://www.archives.gov/federal-register/executive-orders/disposition.html.)

Presidential Memorandum
National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated 21 November 2012 (Available at https://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand.)

UCMJ, Article 106(a)
Espionage

UCMJ, Article 107
False statements

18 USC
Crimes and Criminal Procedure

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate (APD) Web site (www.apd.army.mil). DD forms are available on the Office of the Secretary of Defense (OSD) Web site (www.dtic.mil/whs/directives/forms/index.htm).

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

DD Form 254
Department of Defense Contract Security Classification Specification

Appendix B
Internal Control Evaluation

B–1. Purpose
The function of this evaluation is to ensure effective implementation of the Army's TARP. The purpose of this evaluation is to provide feedback to unit commanders regarding compliance with the training and reporting procedures specified in this regulation.

B–2. 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).

B–3. Test questions
Have Army commanders——

a. Established procedures to ensure that TARP training is scheduled for members of their unit?

b. Included the requirements of this regulation as a mandatory subject in the organizational inspection program?

c. Established a process to track TARP training in their units?

d. Established a process to track TARP training on their installation, if appropriate?

e. Maintained contact information for the supporting CI unit (identity of office, names of CI agents, phone numbers, and e-mail addresses)?

f. Have counterintelligence unit commanders——

g. Established procedures for the preparation and conduct of threat awareness training?

h. Established a professional, relevant, and timely Threat Awareness Program as a priority for the unit's mission of developing CI leads?

i. 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?

j. Included threat awareness and reporting in the Organizational Inspection Program?

k. Coordinated with other intelligence, law enforcement, and force protection agencies to acquire threat data for inclusion in threat awareness training?

l. Established a Covering Agent Program which includes threat awareness training, special threat awareness training, and debriefings?

m. 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?

n. Maintained a calendar for scheduling future training on threat awareness?

o. Maintained contact information on each supported organization?

p. Submitted a quarterly report on the unit's awareness program as required by paragraph 6–2?

q. Submitted CI incident reports within 72 hours after the interview of the person or persons who reported the incident?

r. Have contracting officers included TARP training and reporting requirements in statements of work and on DD Form 254?

B–4. Supersession
This is the initial checklist for the Threat Awareness and Reporting Program.

B–5. Comments
Help make this a better tool for evaluating internal controls. Submit comments to the DCS, 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

ALMS
Army Learning Management System

AOR
area of responsibility

AR
Army regulation

ARNG
Army National Guard

ASCC
Army service component command

ATCICA
Army Theater Counterintelligence Coordinating Authority

CAR
Chief, Army Reserve

CI
counterintelligence

CICA
Counterintelligence Coordinating Authority

CIR
counterintelligence incident report

CNGB
Chief, National Guard Bureau

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

DODD
Department of Defense directive

DODI
Department of Defense instruction

DRU
direct reporting unit

FBI
Federal Bureau of Investigation

FORSCOM
U.S. Army Forces Command

INSCOM
U.S. Army Intelligence and Security Command

JPAS
Joint Personnel Adjudication System

MI
military intelligence

MOS
military occupational specialty

NATO
North Atlantic Treaty Organization

OCONUS
outside the continental United States

RDA
research, development, and acquisition

SAP
Special Access Program

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

USAR
U.S. Army Reserve

USASOC
U.S. Army Special Operations Command

USC
United States Code

USSS
U.S. Secret Service

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 (see AR 525–13).

computer Web-based alternative training
A generic online training tool hosted by ALMS that may be used as an alternate means of receiving TARP training when live training is not possible.

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.

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.

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.

counterterrorism
Offensive measures taken to prevent, deter, and respond to terrorism.

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.

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.

foreign diplomatic establishment
Any embassy, consulate, or interest section representing a foreign country.

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.

leak
The unauthorized disclosure of classified or sensitive information, as to the news media.

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.

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 a CI badge and credentials.

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.

stand alone briefing tool
A multimedia presentation to facilitate live TARP training that may be modified by certified trainers so that portions of it are relevant to target audiences.

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.

suspicious activity
Any behavior that is indicative of criminal activities, intelligence gathering, or other preoperational planning related to a security threat to DOD interests.

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 as possible, report it.

Section III
Special Abbreviations and Terms

ACCA
Allied Counterintelligence Coordinating Authority

ACOP
Army Counterintelligence Operations Portal

agent of a foreign power
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; and/or (5) Knowingly conspires with any person to engage in such activities. Also, 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; and/or (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.

CBT
computer Web-based alternative training

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.

Department of the Army 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.

SBT
stand alone briefing tool

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

T3
train the trainer

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.