

Extract from AR 381-12

Threat Awareness and Reporting Program—4 October 2010

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

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 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	• 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	• 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.

Table 3–1—Indicators of espionage (continued)

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.

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.