

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	<ul style="list-style-type: none"> <li>• Frequent or regular contact with foreign persons from countries which represent an intelligence or terrorist threat to the United States.</li> <li>• Unauthorized visits to a foreign embassy, consulate, trade, or press office, either in CONUS or OCONUS.</li> <li>• Unreported contact with foreign government officials outside the scope of one's official duties.</li> <li>• Business connections, property ownership, or financial interests in a foreign country, excluding the ownership of mutual funds or like investments in foreign companies.</li> <li>• Sending large amounts of money to persons or financial institutions in foreign countries.</li> <li>• Receiving financial assistance from a foreign government, person, or organization.</li> </ul>
Disregard for security purposes	<ul style="list-style-type: none"> <li>• Discussing classified information in unauthorized locations or over a non-secure communications device.</li> <li>• Improperly removing security classification markings from documents and computer media.</li> <li>• Requesting witness signatures on classified document destruction forms when the witness did not actually observe the destruction.</li> <li>• 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.</li> <li>• Repeated involvement in security violations.</li> <li>• Removing, downloading, or printing classified data from DOD computer systems without approval to do so.</li> </ul>
Unusual work behavior	<ul style="list-style-type: none"> <li>• Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities.</li> <li>• 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.</li> <li>• Using copy, facsimile machines, document scanners, or other automated or digital equipment to reproduce or transmit classified material which appears to exceed job requirements.</li> <li>• Repeatedly performing non required work outside of normal duty hours, especially if unaccompanied.</li> <li>• "Homesteading" (requesting tour of duty extensions in one assignment or location), when the assignment offers significant access to classified information.</li> <li>• Manipulating, exploiting, or hacking Government computer systems or local networks to gain unauthorized access.</li> </ul>

**Table 3-1  
Indicators of espionage—Continued**

Behaviors	Indicators
Financial matters*	<ul style="list-style-type: none"> <li>• Unexplained or undue affluence without a logical income source.</li> <li>• Free spending or lavish display of wealth which appears beyond normal income.</li> <li>• A bad financial situation that suddenly reverses, opening several bank accounts containing substantial sums of money, or the repayment of large debts or loans.</li> <li>• Sudden purchases of high value items where no logical income source exists.</li> <li>• Attempts to explain wealth as an inheritance, gambling luck, or a successful business venture, without facts supporting the explanation.</li> </ul>
Foreign travel*	<ul style="list-style-type: none"> <li>• Frequent or unexplained trips of short duration to foreign countries.</li> <li>• Travel that appears unusual or inconsistent with a person's interests or financial means.</li> </ul>
Undue interest	<ul style="list-style-type: none"> <li>• Persistent questioning about the duties of coworkers and their access to classified information, technology, or information systems.</li> <li>• An attempt to befriend or recruit someone for the purpose of obtaining classified or unclassified information.</li> </ul>
Soliciting others	<ul style="list-style-type: none"> <li>• Offers of extra income from an outside venture to those with sensitive jobs or access.</li> <li>• Attempts to entice coworkers into criminal situations which could lead to blackmail or extortion.</li> <li>• Requests to obtain classified information to which the requestor is not authorized access.</li> </ul>

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.