DoD Directive 5240.06
Counterintelligence Awareness and Reporting
Enclosure 4

REPORTABLE CONTACTS, ACTIVITIES, INDICATORS, AND BEHAVIORS.

Table 1. Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors

Table 1. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 22 are subject to punitive action in accordance with section 2 of this enclosure. The activities in items 23 and 24 are reportable, but failure to report these activities may not alone serve as the basis for punitive action.

1. When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems. This includes contact through SNS that is not related to official duties.
2. Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
3. Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
4. Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.
5. Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.
6. Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.
7. Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.
8. Discovery of suspected listening or surveillance devices in classified or secure areas.
9. Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
10. Discussions of classified information over a non-secure communication device.
11. Reading or discussing classified or sensitive information in a location where such activity is not permitted.
12. Transmitting or transporting classified information by unsecured or unauthorized means.
13. Removing or sending classified or sensitive material out of secured areas without proper authorization.
14. Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
15. Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.

16. Improperly removing classification markings from documents or improperly changing classification markings on documents.
17. Unwarranted work outside of normal duty hours.
18. Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
19. Attempts to entice DoD personnel or contractors into situations that could place them in a compromising position.
20. Attempts to place DoD personnel or contractors under obligation through special treatment, favors, gifts, or money.
21. Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
22. Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet or SNS.
23. Trips to foreign countries that are: a. Short trips inconsistent with logical vacation travel or not part of official duties. b. Trips inconsistent with an individual's financial ability and official duties.
24. Unexplained or undue affluence. a. Expensive purchases an individual's income does not logically support. b. Attempts to explain wealth by reference to an inheritance, luck in gambling, or a successful business venture. c. Sudden reversal of a bad financial situation or repayment of large debts.

Table 2. Reportable International Terrorism Contacts, Activities, Indicators, and Behaviors

Table 2. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 9 are subject to punitive action in accordance with section 2 of this enclosure. The activity in item 10 is reportable, but failure to report this activity may not alone serve as the basis for punitive action.

1. Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
2. Advocating support for a known or suspected international terrorist organizations or objectives.
3. Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
4. Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
5. Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
6. Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
7. Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.

8. Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
9. Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.
10. Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

Table 3. Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors

Table 3. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 10 are subject to punitive action in accordance with section 2 of this enclosure. The indicators in items 11 through 19 are reportable, but failure to report these indicators may not alone serve as the basis for punitive action.

1. Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
2. Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3. Network spillage incidents or information compromise.
4. Use of DoD account credentials by unauthorized parties.
5. Tampering with or introducing unauthorized elements into information systems.
6. Unauthorized downloads or uploads of sensitive data.
7. Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8. Downloading or installing non-approved computer applications.
9. Unauthorized network access.
10. Unauthorized e-mail traffic to foreign destinations.
11. Denial of service attacks or suspicious network communications failures.
12. Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13. Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14. Data exfiltrated to unauthorized domains.
15. Unexplained storage of encrypted data.
16. Unexplained user accounts.
17. Hacking or cracking activities.
18. Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19. Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.