



Foreign Influence

- Undisclosed visits to foreign diplomatic facilities
- Trips to foreign countries inconsistent with an individual's financial ability
- Foreign entities targeting employees traveling overseas via airport screening or hotel room incursions
- Unreported close and continuing contact with a foreign national, including intimate contacts, shared living quarters, or marriage

Suspicious Contacts

- Requests for information that make an individual suspicious, including questionable contacts or interaction

Suspicious Financial Activity

- Unexplained expensive purchases not reasonably supported by the individual's income
- Sudden unexplained reversal of a negative financial situation or repayment of large debts

Recording Devices

- Unauthorized possession of cameras or recording or communication devices in classified areas
- Discovery of suspected surveillance devices in classified areas

Cleared Industry's Role

The technology and information resident in U.S. cleared industry is under constant and pervasive threat from foreign intelligence entities seeking to gain the technological edge. Increased awareness of the targeted information and methods of operation used by foreign entities is critical to improving our ability to identify and thwart collection attempts.

Timely and accurate reporting from cleared industry is the primary tool DSS uses to identify and mitigate collection efforts targeting information and technology resident in cleared industry.

Be Alert! Be Aware!

Report suspicious activity to your local security official.



Reporting the Threat



Defense Security Service
Counterintelligence Directorate
www.dss.mil

REPORTING THE THREAT

Reporting Requirements for Cleared Companies

National Industrial Security Program Operating Manual (NISPOM) paragraph 1-302b states, "Contractors shall report efforts by an individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee."

Report actual, probable, or possible espionage, sabotage, terrorism, or subversion promptly to the Federal Bureau of Investigation (FBI) and the Defense Security Service (DSS) (NISPOM 1-301).

Although this requirement is not directed to unclassified information or systems, contractors must report activities that otherwise meet the threshold for reporting, including activities that may have occurred on its unclassified information systems. (See Industrial Security Letter 2013-05)

What to Report*



*** Note:** *Note: Report any of the following incidents if they meet the thresholds of NISPOM paragraphs 1-301, or 1-302a. or b. These lists are not all inclusive. Some of the examples are also considered security violations or personnel security issues, which should be handled in accordance with applicable procedures.

Mishandling of Classified Information

- Removing or sending classified material out of secured areas without proper authorization
- Unauthorized copying, printing, faxing, emailing, or transmitting classified material
- Transmitting or transporting classified information by unsecured or unauthorized means
- Unauthorized storage of classified material, including storage at home
- Reading or discussing classified information in an unauthorized area or over a non-secure communication device
- Improperly removing or changing classification markings
- Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities

Misuse of Computer Systems

- Unauthorized network access
- Unauthorized email traffic to foreign destinations
- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading
- Use of Department of Defense account credentials by unauthorized parties
- Unexplained storage of encrypted data
- Network spillage incidents or information compromise
- Unauthorized transmissions of classified or controlled unclassified information

- Data exfiltrated to unauthorized domains affecting classified information, systems or cleared individuals
- Actual or attempted unauthorized access into U.S. automated information systems
- Tampering with or introducing unauthorized elements into information systems
- Unexplained user accounts, administrator accounts, and expansion of network privileges

Suspicious Cyber Incidents

- Advanced techniques and/or advanced evasion techniques, which imply a sophisticated adversary
- Pre-intrusion aggressive port scanning
- Denial-of-service attacks or suspicious network communication failures
- Social engineering, electronic elicitation, email spoofing, spear phishing, whale phishing, or direct questioning, such as through social networking sites
- Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration
- Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage
- Any cyber activity linked to the law enforcement or counterintelligence suspicious indicators provided by the FBI, DSS, Defense Intelligence Agency or by any other cyber centers