LIS SOLUTIONS

SECURITY MONTHLY NEWSLETTER

DECEMBER 2024

COUNTERINTELLIGENCE AWARENESS

Counterintelligence awareness is crucial because it helps identify various threats from foreign intelligence entities, other illicit collectors of U.S. defense information, and/or terrorists.

What is Counterintelligence?

Counterintelligence is defined as "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities" according to the Executive Order 12333 as amended.

Core Concerns of Counterintelligence

In addition to collecting and processing intelligence about our enemies, the Intelligence Community is also faced with the problem of identifying, understanding, prioritizing, and counteracting the foreign intelligence threats that are encountered by the United States. This activity is known as counterintelligence. The core concerns of counterintelligence are the intelligence from entities of foreign states and similar organizations of non-state actors, such as terrorist organizations and the trusted insider.

The First Line of Defense

You are the first line of defense! Remember, that counterintelligence involves more than simply the catching of adversaries. It involves with understanding, and possibly neutralizing, all aspects of the intelligence operations of foreign nations.

You are the Target

The United States Government relies on you to protect national security by reporting any suspicious behavior that you observe that may be related to a potential compromise of sensitive information. In the eyes of adversaries, there are few true "friends." Only temporarily coinciding interests keep countries cooperating. A rule of thumb, assume that all Foreign Intelligence Entities pose a threat to you and the United States. Finally, remember that your family, friends, and co-workers may be viewed as a means to gain information about you. Report suspicious behavior to your security professionals at security@lissol.com or DoD Hotline at 800-424-9098.

What are the Adversaries Goals?

Foreign entities are actively engaged in efforts to gain information from the United States and its allies. Adversaries try to defeat the United States objectives and advance their interests. Adversaries also attempt to collect information about our plans, our technologies, our activities, and our operations. In addition, adversaries attempt to manipulate and distort the facts of intelligence that we gather. Adversaries seek to detect, disrupt, and counter our national security operations. Finally, adversaries wish to acquire technology that will enhance their capabilities or economic well-being. If these adversaries can learn our methods of operation, then they will be in a better position to carry out their plans to fight against the U.S.

What does the Enemy Want?

Defense Information!!! This includes classified and unclassified information, locations of sensitive information and technology, security weaknesses at cleared facilities and personnel weaknesses that may be exploited.

Collection and Recruitment Methods

- Elicitation is a form of social engineering. It is the process of subtly drawing forth and collecting information from people, through a seemingly innocent conversation. Foreign Intelligence Entities frequently use elicitation to extract information from people who have access to classified or sensitive information.
- Unsolicited Requests for Information is a request for information that was not sought or encouraged by DOD for information from a known or unknown company, or from another country. They may originate via e-mail, telephone, social media or mail. The explosive growth of the Internet and abundance of free e-mail accounts has resulted in increased cases involving suspicious Internet activity.
- Foreign visitors include one-time visitors, long-term visitors such as exchange employees, official government representatives, foreign sales representatives and students. Some indicators of suspicious conduct are:
  - Last-minute and unannounced persons added to the visiting party
  - Wandering visitors who act offended when confronted
  - A Foreign entity attempts a commercial visit or uses a U.S.-based third party to arrange a visit after an original foreign visit request is denied
  - Visitors claim business-related interest but lack experience researching and developing technology
  - Visitors ask to meet personnel from their own countries and attempt to establish continuing contact with them
  - Requests for information outside the scope of what was approved
  - Visitors or students requesting information and becoming irate upon denial
  - Cameras and/or video equipment brought into areas where no photographs are allowed
- Cyber Activities technological advances have made simple mistakes costly to information systems. The malicious insider (disgruntled employee, saboteur, or co-opted employee) has the capability to disrupt interconnected DOD information systems. Other inadvertent actions such as using easy passwords, practicing poor computer security, and emailing or placing personal files on your computer can provide Foreign Intelligence entities an avenue of penetration into DOD systems. Aided by a team of highly sophisticated and well-resourced outsiders, the severity of malicious insider activity may be significantly amplified by: inputting falsified, corrupted data, introducing malicious code such as a virus, logic, or Trojan horse, hacking (also achieved via wireless or Bluetooth), chat rooms, elicitation and relation building, and phishing. All of these actions can potentially reduce or compromise our effectiveness and place the lives of our men and women in jeopardy.

Penalties for Espionage

The penalties for Espionage include:

- Fines
- Up to life imprisonment, and
- Death

Penalties for Theft of Trade Secrets for a Foreign Government

According to the Economic Espionage Act of 1996, the penalties for economic espionage can be stiff. Those using stolen trade secrets to benefit a foreign government face a fine of up to $500,000 and/or up to 15 years in Federal prison, while companies can be fined up to $10 million for stealing trade secrets for another government.

Penalties for Theft of Trade Secrets for Personal Gain

Those who steal trade secrets for their own gain may be fined and/or put in prison for up to ten years. Companies can be fined up to $5 million for using stolen secrets for their own gain.

LIS Solutions
Analyze. Inform. Empower.
718-237-8919 • info@lissol.com