Counterintelligence Awareness and Reporting Course

Student Guide

October 2024

Center for Development of Security Excellence

Contents

Introduction

Introduction

Welcome

Welcome to the DOD Counterintelligence Awareness and Reporting Briefing. This briefing is unclassified.

Introduction

On September 11th, 2001, American Airlines Flight 77 left Washington Dulles International Airport enroute to Los Angeles with a six-person crew and 58 passengers. Five of those passengers were terrorists, who hijacked the plane and intentionally crashed it into the Pentagon. The attack on the Pentagon killed 184 people. The Department of Defense, or DOD, is the target of both foreign intelligence threats and potential terrorist attacks. On any given day, a foreign intelligence entity or terrorist may be assessing a DOD employee for recruitment to commit espionage or acts of terrorism. We must remain vigilant in recognizing and reporting signs of espionage and terrorism.

Objectives

At the conclusion of this briefing, you will be able to:

- Explain the role each individual plays in counterintelligence
- Summarize the threats posed by foreign intelligence entities
- Recognize collection methods used by foreign intelligence entities to obtain information
- Recognize recruitment efforts of foreign intelligence entities
- Describe the potential threat posed by trusted insiders
- List Potential Espionage Indicators (PEI)
- List warning signs and indicators of potential terrorism
- List the reporting requirements for PEI and Anomalous Health Incidents (AHI)

Module 1

What is Counterintelligence?

What is Counterintelligence?

Counterintelligence, or CI, as defined by Executive Order 12333, as amended, is "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."

The National Counterintelligence Strategy of the U.S. states that "CI includes defensive and offensive activities conducted at home and abroad to protect against the traditional and emerging foreign intelligence threats of the 21st century."

Core Concerns of Counterintelligence

In addition to collecting and processing intelligence about our enemies, the Intelligence Community, or IC, is also faced with the challenge of identifying, understanding, prioritizing, and counteracting foreign intelligence threats to the United States. This activity is known as CI.

The core CI concerns are the intelligence entities of foreign states and 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 CI is more than just catching spies. It is, in fact, concerned with understanding, and possibly neutralizing, all aspects of the intelligence operations of foreign nations.

You Are The Target

The government relies on you to protect national security by remaining vigilant, observant, and ready to report activity potentially related to the compromise of sensitive information. In the espionage game, there are few true "friends", only coinciding interests.

ALL foreign intelligence entities can pose threats. Most foreign governments still place a high priority on U.S. Government information, despite the end of Cold War.

As a DOD employee, you can be the target of a foreign intelligence entity anytime, anywhere because of:

- What you have access to
- Who you have access to
- What you know

Remember, family, friends, and co-workers may be viewed as a means to gain information about you.

ALWAYS REPORT SUSPICIOUS BEHAVIOR to your unit security or CI office.

Foreign Intelligence Entity Threats

The threat isn't just foreign intelligence officers; it is also from hackers, criminal elements, and insiders who wittingly or unwittingly aid our adversaries. Both foreign countries and domestic competitors may attempt to collect information on critical technologies from DOD personnel or contractors. The use of discretion and basic CI awareness can protect you against foreign intelligence entity attempts to collect classified, unclassified, or sensitive information.

Economic Espionage Annual Loss

According to the Assistant Director of the FBI's counterintelligence CI division, in 2015 there was a 53% increase in economic espionage cases, leading to the loss of hundreds of billions of dollars. This number increases yearly.

Knowledge Check

Knowledge Check 1

Can you solve this puzzle?

Select the best response for each question. Check your answers in the Answer Key at the end of this Student Guide.

CI includes only offensive activities.

- ○ True
- ○ False

Knowledge Check 2

CI is concerned with understanding, and possibly neutralizing, all aspects of the intelligence operations of foreign nations.

- ○ True
- ○ False

Knowledge Check 3

As a DOD employee, you can be the target of a foreign intelligence entity.

- ○ True
- ○ False

Knowledge Check 4

Family, friends, and co-workers may be used as a means to gain information about you.

- ○ True
- ○ False

Knowledge Check 5

This former U.S. Nuclear Regulatory Commission employee pled guilty to attempted spear-phishing cyber-attack on Department of Energy Computers.

Just for fun, guess who this person is. This is not a test!

- ○ Robert Hanssen
- ○ Charles Eccleston
- ○ Edward Snowden
- ○ Mostafa Awwad

Module 2

Understanding our Adversaries

What are the Adversaries' Goals?

Foreign entities are actively engaged in efforts to gain information from the U.S. and its allies. To defeat our objectives and advance their interests, they attempt to collect information about our plans, technologies, activities, and operations.

They conduct overt and covert influence operations to manipulate and distort the truth, to include the intelligence we collect and the information the public consumes.

Foreign intelligence entities seek to detect, disrupt, and counter our national security operations. In addition, they wish to acquire technology that will enhance their capabilities or economic well-being.

If they can learn our Methods of Operation, or MOs, they will be in a better position to carry out their plans.

Threats to Industry

Foreign intelligence entities view the Defense Industrial Base as a target for exploitation, manipulation, disruption, and most commonly theft via industrial espionage.

Since the DOD relies on the cleared defense contractors developing our nation's classified or most critical technologies, that puts DOD in the same cross hairs. Our adversaries are highly sophisticated, constant, and pervasive.
Regardless of the method or activity, foreign intelligence entities seek one thing: to learn more about the DOD plans in order to exploit its information and impede its mission.

Foreign Intelligence Threats

Traditional activity includes:

- Foreign intelligence entities operating out of:
  - Embassies
  - Consulates
  - Universities
  - Trade Missions
- Foreign intelligence entity use of Insiders (Insider Threat)

Non-traditional activity includes:

- Foreign government-sponsored commercial enterprises
- International trafficking organizations
- Terrorist organizations

What Do They Want?

What do they want? National Defense Information.

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

Intelligence Collection Tradecraft

Many nations' intelligence organizations target defense information, and they will do all they can to obtain it. As government employees and contractors, our greatest vulnerabilities are those things we take for granted. For example, foreign intelligence entities use:

- Intercepts of cell phone signals
- Exploitation of public or otherwise unsecured wireless networks
- Intercepts of open telephone lines
- Intercepts in hotels while on a Temporary Duty Station (TDY)
- Looking through the trash
- Simple conversations, online or in person
- Hacking into unclassified or classified systems

Knowledge Check

Knowledge Check 1

Can you solve this puzzle?

Select the best response for each question. Check your answers in the Answer Key at the end of this Student Guide.

To defeat our objectives and advance their interests, foreign entities attempt to collect information about our plans, technologies, activities, and operations.

○ True

- ○ False

Knowledge Check 2

Traditional espionage activity includes foreign government-sponsored commercial enterprises, international trafficking organizations, and terrorism.

- ○ True
- ○ False

Knowledge Check 3

Inadvertent actions, such as using easy passwords and practicing poor computer security, can provide foreign entities an avenue to penetrate DOD systems.

- ○ True
- ○ False

Knowledge Check 4

As government employees, our greatest vulnerabilities are those things we take for granted.

- ○ True
- ○ False

Knowledge Check 5

This Navy Civilian Engineer shared the schematics of the USS Gerald R. Ford nuclear aircraft with individuals whom he believed were representing a foreign government.

Just for fun, guess who this person is. This is not a test!

- ○ Yuan Li
- ○ Walter Liew
- ○ Robert Mo
- ○ Mustafa Awwad

Module 3

Collection and Recruitment Methods

Collection Methods

Some MOs frequently used by Foreign Intelligence to collect information include:

- Elicitation
- Unsolicited requests for information
- Foreign visits to DOD installations or facilities
- International conventions, seminars, and exhibits
- Solicitation and marketing of services
- Academic solicitation
- Cyber activities
- Open source

Elicitation

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

An unsolicited request for information is any request that was not sought or encouraged by DOD for information from a known or unknown company, or from another country. They may originate via email, 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 Visits

Foreign visits 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 claiming business-related interest but lack experience researching and developing technology
- Visitors asking 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
- Hidden agendas NOT associated with the stated purpose of the visit
- Visitors or students requesting information and becoming irate upon denial
- Cameras and/or video equipment brought into areas where no photographs are allowed

The names of all foreign visitors to your unit facility or installation must be approved prior to the visit. It is important to note that not all foreign visitors are intelligence officers. However, some are here to collect more information than they are legally allowed.
Contact your CI or security official immediately upon learning that you will be the host of a foreign visit. CI specialists can provide foreign threat and awareness briefings and possible countermeasures. Protect your work environment and any classified or sensitive information you may be working on when foreign visitors are in your workspace.

International Conventions, Seminars, and Exhibits

Although the monitoring of telephones and hotel room intrusions are not as likely to take place within the continental United States, this does not preclude a hostile entity from developing and exploiting a relationship with hotel employees. Technical experts may receive invitations to share their knowledge in international forums or could be "pressed" for restricted, proprietary, and classified information.

Some indicators of this collection practice are:

- Conversations involving classified, sensitive, or export-controlled technologies or product

- The foreign country or organization hosting the event unsuccessfully attempted to visit U.S. government installations or facilities in the past
- You receive an all-expense-paid invitation to lecture in a foreign nation
- Entities want a summary of the requested presentation or brief several months prior to the lecture date
- Excessive or suspicious photography and filming of technology and products
- Casual conversations during and after the event hinting at future contacts or relations
- Foreign attendees' business cards do not match stated affiliations

Solicitation and Marketing of Services

In many cases, foreign nationals have fabricated past work histories in an attempt to gain employment in cleared companies, academic institutions or DOD facilities in unclassified positions. Some indicators of this collection method include:

- Invitations for cultural exchanges, individual-to-individual exchanges, or ambassador programs
- Offers to act as a sales or purchasing agent in foreign countries
- Internships sponsored by a foreign government or foreign business
- Purchases of foreign-made equipment

It is your responsibility to ensure that any contact you have with a foreign national or entity in the course of your duties has been thoroughly evaluated by your agency security officials.

Academic Solicitation

Academic solicitation is a method in which foreign intelligence entities use students, professors, scientists or researchers as collectors. These individuals are recruited to improperly attempt to obtain sensitive or classified information. Requests may originate from known or unknown sources including:

- Foreign universities or academic centers
- Individuals overseas or placed in the U.S.
- Quasi-governmental organizations such as research centers and institutes

There are several situations which may be an indication of attempted academic solicitation:

- A foreign student who has been accepted to a U.S. university or postgraduate research programs may be recruited by their home country to collect information.
    - They may be offered state-sponsored scholarships as an incentive for their collection efforts.
- U.S. researchers may receive:
    - Requests to provide dual-use components under the guise of academic research.
    - Unsolicited emails from peers in their academic field soliciting assistance on fundamental and developing research.
- Overqualified candidates who seek to work in cleared laboratories as interns may indicate an attempt at Academic Solicitation.
- Other attempts may occur when candidates seeking to work in cleared laboratories in areas of study incompatible with the requesting individual's field of research.
- Intelligence entities may also send subject matter experts (SMEs) requests to review research papers.

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 insider malicious activity may be significantly amplified by: inputting falsified, corrupted data, malicious code (for example, virus, logic, Trojan horse), hacking, also achieved via wireless or Bluetooth, chat rooms – elicitation, relation building, and phishing. All of

these actions can potentially reduce or compromise our effectiveness and place in jeopardy the lives of our men and women.

Open Source

Foreign intelligence entities also collect information from publicly available sources. Examples of open sources of information include:

- Online sources
- Online and physical publications, such as:
  - Magazines
  - Journals
  - Newspapers
- Visual content, such as:
  - Movies
  - Television
- Audio content, such as:
  - Podcasts
  - Radio
  - Interviews
- Online communities and user-generated content, such as:
  - Social Networking sites
  - Video sharing sites
  - Wikis
  - Blogs
- Government reports, such as:
  - Budgets
  - Demographics
  - Hearings
  - Legislative debates
  - Press conferences
  - Speeches which often contain information of interest to our adversaries.

- Corporate or business websites can also be used to gather the open source information. Corporate financial information can also be collected from sites like Reuters or Dunn & Bradstreet.
- Amateur airplane spotters, radio monitors and satellite observers have provided significant information not otherwise available. The availability of worldwide satellite photography on the Web, like Google Earth, has expanded open source capabilities into areas formerly available only to major intelligence services
- Professional and academic conferences, symposia, professional associations, academic papers, and subject matter experts may also be open sources of intelligence information

Reportable Suspicious Activity

According to DOD DIRECTIVE NUMBER 5240.06 titled "Counterintelligence Awareness and Reporting (CIAR)" Reportable foreign intelligence entity-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors include:

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 USB, 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.

Recruitment versus Volunteers

A Personnel Security Research Center study revealed that two thirds of those convicted in recent espionage cases were volunteers. But that still means that in one third of all espionage cases, a trusted insider with placement and access was recruited to collect and transmit protected information.

Recruitment Process

The recruitment process can be broken down into five phases and may take up to three years to develop. Please note that the recruitment process has an end stage, Termination, that is not discussed in this course.

Spotting

In the Spotting phase the foreign intelligence officer identifies the target. The intelligence officer may begin by accessing the corporate web page to identify candidates to target via emails or social engineering.

Assessing

In the Assessing phase the foreign intelligence officer will look for exploitable weaknesses such as: alcohol abuse, drug use, extramarital affairs, gambling or other financial problems.

Developing

In the Developing phase, the foreign intelligence officer attempts to establish a close relationship with the target. Once established, the foreign intelligence officer makes an offer to help the target with his problems.

Recruiting

If the target takes the bait, the foreign intelligence officer recruits the target to move into a more clandestine relationship.

Handling

In the Handling phase, the foreign intelligence officer will instruct the target on specific information needed. The foreign intelligence officer begins paying the target for his efforts. The target is now hooked and on his way to commit espionage.

Knowledge Check

Knowledge Check 1

Can you solve this puzzle?

Select the best response for each question. Check your answers in the Answer Key at the end of this Student Guide.

Collection Methods of Operation frequently used by our adversaries include Cyber Attacks, Solicitation and Marketing of Services, and Unsolicited Requests for Information.

- ○ True
- ○ False

Knowledge Check 2

Foreign entities are overt in their collection methods and do not use subtle techniques such as elicitation.

- ○ True
- ○ False

Knowledge Check 3

The “Spotting” phase is the initial step in the recruitment process.

- ○ True
- ○ False

Knowledge Check 4

Cyber vulnerabilities to DOD Systems may include illegal downloads, weak passwords, and viruses.

- ○ True
- ○ False

Knowledge Check 5

This U.S. Navy sailor accepted $11,500 from an undercover FBI agent posing as a Chinese intelligence officer in exchange for information, documents, photographs, and images that were classified as secret or top secret.

Just for fun, guess who this person is. This is not a test!

- ○ Kun Shan Chun
- ○ Bryan Martin
- ○ Bryan Underwood
- ○ Wen Chyu Liu

Module 4

Indicators

Indicators of Foreign Intelligence Entity Targeting

Some indicators of foreign intelligence entity targeting are:

- Being invited to lecture or attend a conference in a foreign country
- Being singled out for socializing or special attention
- Meeting a foreign national and becoming romantically involved, and
- Becoming personally involved with a known or suspected foreign intelligence officer or foreign intelligence entity

Potential Espionage Indicators

Potential espionage indicators, or PEIs, are activities, behaviors, or circumstances that "may be indicative" of potential espionage activities by an individual who may have volunteered or been recruited by a foreign intelligence entity as a witting espionage agent.

Many of these methods result in detectable behavior and activities that could indicate an act of espionage. Some potential indicators are:

- Unexplained affluence
- Concealing foreign travel
- Unusual interest in information outside the scope of assigned duties
- Unusual work hours
- Taking classified material home
- Disgruntled
- Copying files
- Unreported contact with foreign nationals
- Attempting to gain access, without need-to-know
- Unexplained absences
- Foreign travel of short duration
- Avoiding polygraph

- Terminating employment
- Unauthorized downloads

These indicators are not limited to those with access to classified information.

What is a Security Anomaly?

Security anomaly: "Foreign power activity or knowledge which is inconsistent with the expected norm that suggests that foreign powers have knowledge of U.S. national security"

Examples of anomalies include:

- An adversary conducts activities with precision that indicates prior knowledge
- An adversary uses technical countermeasures to block a previously undisclosed or classified U.S. intercept technology
- Foreign officials reveal details they should not have known
- An adversary is able to anticipate DOD plans and activities
- Media is waiting where a sensitive DOD program will be tested

Detection and Identification

Detecting an anomaly requires a degree of suspicion. Don't simply believe that the unexpected activity was coincidental. Anything that doesn't fit the pattern could be an indicator of espionage. When in doubt, report it!

Knowledge Check

Knowledge Check 1

Can you solve this puzzle?

Select the best response for each question. Check your answers in the Answer Key at the end of this Student Guide.

PEIs are activities, behaviors, or circumstances that "may be indicative" of potential espionage activities.

○ True

○ False

Knowledge Check 2

A Security Anomaly is foreign power activity or knowledge inconsistent with the expected norm that suggests knowledge of U.S. national security.

- ○ True
- ○ False

Knowledge Check 3

Being invited to lecture/attend a conference in a foreign country is one potential indicator of foreign entity targeting.

- ○ True
- ○ False

Knowledge Check 4

Most unexpected activity isn't espionage; you should only report things that are obviously indicators of espionage.

- ○ True
- ○ False

Knowledge Check 5

This former U.S. Consulate Guard was sentenced to nine years in prison for attempting to communicate national defense information to China for personal financial gain.

Just for fun, guess who this person is. This is not a test!

- ○ Charles Eccleston
- ○ Bryan Martin
- ○ Christopher Boyce
- ○ Bryan Underwood

Module 5

Terrorism and Force Protection

Terrorism

As you may recall, the definition of counterintelligence included international terrorist organizations or activities. Unfortunately, acts of terrorism are an all-too common fact of modern life.

Who can forget the December 3, 2015, attack in San Bernardino, California where shots rang out fire at the Inland Regional Center and 14 people were killed by Syed Rizwan Farook and Tashfeen Malik.

On June 12, 2016, an American-born man who had pledged allegiance to ISIS gunned down 49 people in a nightclub in Orlando, Florida.

On July 16, 2015, a lone gunman shot and killed four Marines during two attacks at military facilities in Chattanooga, Tennessee.

All of these terrorist events have one thing in common - they were inspired by a foreign entity intent on harming America. These “state-sponsored” terror attacks are well-known and their costs are devastating.

Workplace Violence

On September 16, 2013, a lone gunman fatally shot twelve people and injured three others in a mass shooting at the headquarters of the Naval Sea Systems Command, or NAVSEA, inside the Washington Navy Yard in southeast Washington, D.C.

Workplace violence is any act or threat of physical violence, harassment, intimidation, or other threatening disruptive behavior that occurs at the work site. It ranges from threats and verbal abuse to physical assaults and even homicide. It can affect and involve employees, clients, customers and visitors. However it manifests, workplace violence is a major concern for employers and employees nationwide.

DOD Instruction 1438.06 requires all components to establish a workplace violence prevention program and to properly investigate and address workplace violence events. Supervisors must immediately report threats of workplace violence to their management and appropriate military or civilian authorities. Your workplace violence program must also ensure that annual training is provided for all employees.

Terrorism Indicators

Perhaps the most famous attacked inspired by a foreign entity happened on April 15, 2013, when two bombs went off near the finish line of the Boston Marathon, killing three spectators and wounding more than 260 other people. Four days later, after an intense manhunt, police captured Dzhokhar Tsarnaev, whose older brother Tamerlan Tsarnaev was killed in a shootout with police earlier in the day. The two bombers did not have any established ties to a foreign entity. They had become self-radicalized and acted without direction. But the results were devastating, nonetheless.

Whether it be foreign inspired terrorism or workplace violence, everyone has a responsibility to be alert for any indications of a threat, regardless of the source. But so called, home-grown terror can best be spotted through tips and reports of unusual activities.

According to DOD DIRECTIVE NUMBER 5240.06 titled "Counterintelligence Awareness and Reporting (CIAR)" reportable international terrorism contacts, activities, indicators, and behaviors include:

- Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization
- Advocating support for a known or suspected international terrorist organizations or objectives
- Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist
- 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
- Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts
- Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same
- Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities

- Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization
- Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters
- 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

Reporting

When it comes to defeating terrorism, the phrase to remember is, "If you see something say something." Report any suspicious or unexplained activity. Trust your instincts; report potential indication of terror activities. Remember, it is not your job to investigate, but it is your responsibility to report it so authorities can.

Knowledge Check

Knowledge Check 1

Can you solve this puzzle?

Select the best response for each question. Check your answers in the Answer Key at the end of this Student Guide.

Potential espionage indicators include: unexplained affluence, concealing foreign travel, unusual work hours, and taking classified material home.

○ True
○ False

Knowledge Check 2

When in doubt about something you see, you should report it to the proper authorities.

○ True
○ False

Knowledge Check 3

If a co-worker asks you for access to material that he doesn't have a need to know, you should report the incident to the proper authorities.

- ○ True
- ○ False

Knowledge Check 4

Counterintelligence operations do not address terrorism.

- ○ True
- ○ False

Knowledge Check 5

This disgruntled, civilian employee was sentenced to 4 consecutive life sentences for the murders of two co-workers at the Coast Guard Base on Kodiak Island, Alaska. A recent court decision has overturned this conviction on technical grounds pending appeal. This person's guilt nor the quality of the investigation was a factor in this decision.

See if you can guess who this is. This is not a test!

- ○ Edward Snowden
- ○ James Wells
- ○ Robert Mo
- ○ Robert Hanssen

Module 6

Responsibilities and Reporting Requirements

Responsibilities and Reporting Requirements

So, what should you do? Everyone has CI responsibilities to keep our nation's secrets and to protect ourselves and our co-workers. Remember, "if you see something, say something." Learn more about your CI responsibilities and the Reporting Requirements for CI-related incidents below.

Responsibilities

If you feel you are being solicited for information:

- Prepare in advance: practice responses to possible questions concerning your duties.
- Never answer questions which make you feel uncomfortable. Without indicating that you are uncomfortable, change any conversation that might be too probing with respect to your duties, private life, and coworkers.
- Be observant: Note as much as possible about the person asking questions.
- Do not probe for information. Nonchalantly ask questions about them.
- Be especially wary of questions about your personal information or colleagues' and provide non-descript answers; leave the talking to someone else.
- Practice good Operations Security, or OPSEC!
- Do not leave sensitive documents or equipment unattended in cars, hotel rooms, or hotel safes.
- Store the information in appropriate secure facilities like a U.S. Military or government site, a U.S. Embassy, U.S. Federal law enforcement office, or a cleared contractor facility.
- Keep unwanted material secured until it can be disposed of.
- Burn or shred paper and discs or other media.
- Practice good Communications Security!

- Do not use personal or commercial computers, or telephones, for sensitive or classified matters, especially at a foreign establishment.
- Take the time to use secure communications equipment at appropriate U.S. Government establishments such as an Embassy, U.S. Federal law enforcement office, or a cleared contractor facility.
- Take the battery out of cell phones before holding sensitive discussions and beware of being overheard in public.
- Ask yourself: Does anyone need to know the information? Is there a need to share the information?

We need to continue working toward establishing and maintaining dissemination and control procedures that balance need-to-know with necessity of sharing classified information. A significant number of individuals convicted of espionage and other national security crimes had access to and later passed information that they had no need-to-know.

Requirements

Everyone is required to report behaviors and indicators of potential foreign intelligence entity threats. DOD personnel should report potential foreign intelligence entity threats and anomalous health incidents (AHI), to their organization's CI element, supporting MDCO or their commander. DOD personnel who fail to report PEI information may be subject to judicial or administrative action, or both. Persons subject to the Uniform Code of Military Justice, or UCMJ, who fail to report may be subject to punitive action under Article 92, UCMJ.

DOD civilians and contractors should report the threat without delay to their Facility Security Officer, or FSO, or Supervisor. Civilian employees and contractors failing to report may be subject to appropriate disciplinary action under regulations governing civilian employees. Non-DOD civilians who fail to report, may face sanctions as outlined in their facility's Security Implementation plan or HR policies.

Anomalous Health Incident

Anomalous Health Incidents (AHI), also known as Havana Syndrome, may cause individuals to experience unexplained sensory events coupled with physical symptoms, including some combination of sounds or sensations of sounds, pressure, vibrations, heat, and/or unexplained physical discomfort such as pain, nausea, and disequilibrium. Symptoms typically include headache, pain, nausea, unsteadiness or a vertigo-like feeling, and

cognitive "fog." Some reported a clear area of effect, where one can move out of the sensation. If you believe you have or are experiencing an AHI, immediately remove yourself, coworkers, and family members from the area, seek any necessary medical attention, and report the event.

Here is some additional information about AHIs. AHIs are NOT fully understood. Suspected AHIs are a mandatory reportable security anomaly. Suspected AHIs can occur worldwide (CONUS and OCONUS). Though the events are rare, timely reporting is vital to investigations, operations, and to a speedy recovery. An affected individual will need to report suspected AHI through their chain of command, security officer, and their CI element as soon as possible. Voluntary debriefs are extremely valuable, and it is encouraged that all government personnel and covered contractors participate in AHI interviews or debriefs.

Penalties for Espionage

Those who commit espionage face severe penalties, including:

- Fines
- Up to life imprisonment
- In some cases, the death penalty

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.

Course Summary

Congratulations! You have completed the *Counterintelligence Awareness and Reporting Course*.

You should now be able to perform all of the listed activities.

- Explain the role each individual plays in counterintelligence
- Summarize the threats posed by foreign intelligence entities
- Recognize collection methods used by foreign intelligence entities to obtain information
- Recognize recruitment efforts of foreign intelligence entities
- Describe the potential threat posed by trusted insiders
- List Potential Espionage Indicators (PEI)
- List warning signs and indicators of potential terrorism
- List the reporting requirements for PEI and Anomalous Health Incidents (AHI)

To receive course credit, you must take and pass the *Counterintelligence Awareness and Reporting Course* examination with a score of 75% or higher. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to access the online exam.

Appendix A: Answer Key

Module 1 Knowledge Checks

Knowledge Check 1

Can you solve this puzzle?

CI includes only offensive activities.

- ○ True
- ⦿ False (correct response)

***Feedback**: CI includes both offensive and defensive activities.*

Knowledge Check 2

CI is concerned with understanding, and possibly neutralizing, all aspects of the intelligence operations of foreign nations.

- ⦿ True (correct response)
- ○ False

***Feedback**: CI is concerned with understanding, and possibly neutralizing, all aspects of the intelligence operations of foreign nations.*

Knowledge Check 3

As a DOD employee, you can be the target of a foreign intelligence entity.

- ⦿ True (correct response)
- ○ False

***Feedback**: As a DOD employee, you can be the target of a foreign intelligence entity, anytime or anywhere.*

Knowledge Check 4

Family, friends, and co-workers may be used as a means to gain information about you.

- ⦿ True (correct response)
- ○ False

***Feedback**: Family, friends, and co-workers may be used as a means to gain information about you. Our adversaries will use any means necessary to get the information they want.*

Knowledge Check 5

This former U.S. Nuclear Regulatory Commission employee pled guilty to attempted spear-phishing cyber-attack on Department of Energy Computers.

Just for fun, guess who this person is. This is not a test!

- ○ Robert Hanssen
- ⊙ Charles Eccleston (correct response)
- ○ Edward Snowden
- ○ Mostafa Awwad

***Feedback**: This is Charles Eccleston. You can read the case study about him in the Course Resources.*

Module 2 Knowledge Checks

Knowledge Check 1

To defeat our objectives and advance their interests, foreign entities attempt to collect information about our plans, technologies, activities, and operations.

- ⊙ True (correct response)
- ○ False

***Feedback**: Foreign entities attempt to collect information about our plans, technologies, activities, and operations in order to defeat our objectives and advance their interests.*

Knowledge Check 2

Traditional espionage activity includes foreign government-sponsored commercial enterprises, international trafficking organizations, and terrorism.

- ○ True
- ⊙ False (correct response)

***Feedback**: Traditional activity includes Foreign Intelligence Entities operating out of: embassies, consulates, universities, and trade missions, spies or their sources, and insider threats.*

Knowledge Check 3

Inadvertent actions, such as using easy passwords and practicing poor computer security, can provide foreign entities an avenue to penetrate DOD systems.

- ⦿ True (correct response)
- ○ False

***Feedback**: Inadvertent actions, such as using easy passwords and practicing poor computer security, can provide foreign entities an avenue to penetrate DOD systems.*

Knowledge Check 4

As government employees, our greatest vulnerabilities are those things we take for granted.

- ⦿ True (correct response)
- ○ False

***Feedback**: As government employees, our greatest vulnerabilities are those things we take for granted.*

Knowledge Check 5

This Navy Civilian Engineer shared the schematics of the USS Gerald R. Ford nuclear aircraft with individuals whom he believed were representing a foreign government.

Just for fun, guess who this person is. This is not a test!

- ○ Yuan Li
- ○ Walter Liew
- ○ Robert Mo
- ⦿ Mustafa Awwad (correct response)

***Feedback**: This is Mustafa Awwad. You can read the case study about him in the Course Resources.*

Module 3 Knowledge Checks

Knowledge Check 1

Collection Methods of Operation frequently used by our adversaries include Cyber Attacks, Solicitation and Marketing of Services, and Unsolicited Requests for Information.

- ⦿ True (correct response)
- ○ False

***Feedback**: Foreign entities use a variety of methods to collect information about our plans, technologies, activities, and operations.*

Knowledge Check 2

Foreign entities are overt in their collection methods and do not use subtle techniques such as elicitation.

- ○ True
- ⦿ False (correct response)

***Feedback**: Foreign Intelligence Entities use a form of social engineering called Elicitation to subtly draw information from people who have access to classified or sensitive information, through a seemingly innocent conversation.*

Knowledge Check 3

The "Spotting" phase is the initial step in the recruitment process.

- ⦿ True (correct response)
- ○ False

***Feedback**: Foreign Intelligence Entities identify a target for potential espionage in the spotting phase.*

Knowledge Check 4

Cyber vulnerabilities to DOD Systems may include illegal downloads, weak passwords, and viruses.

- ⦿ True (correct response)
- ○ False

***Feedback**: These vulnerabilities can potentially reduce or compromise your network security and place in jeopardy our classified or sensitive information.*

Knowledge Check 5

This U.S. Navy sailor accepted $11,500 from an undercover FBI agent posing as a Chinese intelligence officer in exchange for information, documents, photographs, and images that were classified as secret or top secret.

Just for fun, guess who this person is. This is not a test!

- ○ Kun Shan Chun

- ⦿ Bryan Martin (correct response)
- ○ Bryan Underwood
- ○ Wen Chyu Liu

***Feedback**: This is Bryan Martin. You can read the case study about him in the Course Resources.*

Module 4 Knowledge Checks

Knowledge Check 1

PEIs are activities, behaviors, or circumstances that "may be indicative" of potential espionage activities.

- ⦿ True (correct response)
- ○ False

***Feedback**: PEIs are activities, behaviors, or circumstances that "may be indicative" of potential espionage activities.*

Knowledge Check 2

A Security Anomaly is foreign power activity or knowledge inconsistent with the expected norm that suggests knowledge of U.S. national security.

- ⦿ True (correct response)
- ○ False

***Feedback**: A Security Anomaly is foreign power activity or knowledge inconsistent with the expected norm that suggests knowledge of U.S. national security.*

Knowledge Check 3

Being invited to lecture/attend a conference in a foreign country is one potential indicator of foreign entity targeting.

- ⦿ True (correct response)
- ○ False

***Feedback**: Being invited to lecture/attend a conference in a foreign country is one potential indicator of foreign entity targeting.*

Knowledge Check 4

Most unexpected activity isn't espionage; you should only report things that are obviously indicators of espionage.

- ○ True
- ⦿ False (correct response)

***Feedback**: While most unexpected activity isn't espionage, indicators are not obvious. You should report all suspicious activity.*

Knowledge Check 5

This former U.S. Consulate Guard was sentenced to nine years in prison for attempting to communicate national defense information to China for personal financial gain.

Just for fun, guess who this person is. This is not a test!

- ○ Charles Eccleston
- ○ Bryan Martin
- ○ Christopher Boyce
- ⦿ Bryan Underwood (correct response)

***Feedback**: This is Bryan Underwood. You can read the case study about him in the Course Resources.*

Module 5 Knowledge Checks

Knowledge Check 1

Potential espionage indicators include: unexplained affluence, concealing foreign travel, unusual work hours, and taking classified material home.

- ⦿ True (correct response)
- ○ False

***Feedback**: Potential espionage indicators include: unexplained affluence, concealing foreign travel, unusual work hours, and taking classified material home.*

Knowledge Check 2

When in doubt about something you see, you should report it to the proper authorities.

- ⦿ True (correct response)
- ○ False

***Feedback**: When in doubt about something you see, you should report it to the proper authorities.*

Knowledge Check 3

If a co-worker asks you for access to material that he doesn't have a need to know, you should report the incident to the proper authorities.

- ⦿ True (correct response)
- ○ False

***Feedback**: If a co-worker asks you for access to material that he doesn't have a need to know, you should report the incident to the proper authorities.*

Knowledge Check 4

Counterintelligence operations do not address terrorism.

- ○ True
- ⦿ False (correct response)

***Feedback**: Counterintelligence operations do address terrorism.*

Knowledge Check 5

This disgruntled, civilian employee was sentenced to 4 consecutive life sentences for the murders of two co-workers at the Coast Guard Base on Kodiak Island, Alaska. A recent court decision has overturned this conviction on technical grounds pending appeal. This person's guilt nor the quality of the investigation was a factor in this decision.

See if you can guess who this is. This is not a test!

- ○ Edward Snowden
- ⦿ James Wells (correct response)
- ○ Robert Mo
- ○ Robert Hanssen

***Feedback**: This is James Wells.*