STUDENT GUIDE

DoD CI AWARENESS AND REPORTING COURSE FOR DoD EMPLOYEES CI116.16

Contents

Course Introduction..3
Objectives 3
What is Counterintelligence?..4
Core Concerns of Counterintelligence 4
The First Line of Defense 4
You are the Target 5
FIE Threats 5
Economic Espionage Annual Loss 5
Understanding Our Adversaries 6
What are the Adversaries Goals?..6
Threats to Industry 6
Foreign Intelligence Threats 6
What do they Want?..7
Intelligence Collection Tradecraft 7
Collection and Recruitment Methods..8
Elicitation..8
Unsolicited Requests for Information..8
Foreign Visits 8
International Conventions, Seminars, and Exhibits..9
Solicitation and Marketing of Services..10
Academic Solicitation 11
Cyber Activities..12
Open Source 12
Reportable Suspicious Activity 13
Recruitment vs. Volunteers..14
Spotting Phase..14
Assessing Phase..15
Developing Phase 15
Recruiting Phase..15
Handling Phase..15
Indicators 16
Indicators of FIE Targeting 16
Potential Espionage Indicators 16
What is a Security Anomaly?..17
Terrorism and Force Protection..18
Terrorism..18
Workplace Violence..18
Terrorism Indicators 19
Responsibilities and Reporting Requirements 21
Responsibilities 21
Reporting..22
Requirements..22
Penalties for Espionage..22
Penalties for Theft of Trade Secrets for a Foreign Government........23
Penalties for Theft of Trade Secrets for Personal Gain....................23

Welcome

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

Course Introduction

On September 11, 2001, American Airlines Flight 77 left Washington Dulles International Airport en-route to Los Angeles with a six-person crew and 58 passengers. Five of those passengers were actually terrorists, who hijacked the plane and intentionally crashed it into the Pentagon. The attack on the Pentagon killed 184 people.

The Department of Defense is the target of both Foreign Intelligence Threats and potential terrorist attacks. On any given day, a foreign intelligence agent 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 (FIE);
- Recognize collection methods used by FIE to obtain information;
- Recognized recruitment efforts of FIE;
- 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.

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 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 CI are the intelligence 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 CI involves more than simply the catching of 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 reporting any behavior that you observe that may be related to a potential compromise of sensitive information. In the spy game there are few true "friends." Only temporarily coinciding interests keep countries cooperating.

ALL Foreign Intelligence Entities can pose threats. Most foreign governments still place a high priority on U.S. Government information, despite the end of the 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; or
- What you know

Remember, family, friends, and co-workers may be viewed as a means to gain information about you. Report suspicious behavior to your unit security or counterintelligence office.

FIE Threats

The threat isn't just foreign intelligence officers, it is also from hackers, criminal elements, and insiders who have agreed to aid our adversaries. Both foreign countries and domestic competitors may attempt to collect information on critical technologies from DoD personnel or contractors. Common sense 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 division, Randall Coleman, 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.

<u>Understanding Our Adversaries</u>

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.

In an attempt to manipulate and distort the facts of intelligence we gather, they may conduct covert influence operations. They 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, they will be in a better position to carry out their plans.

Threats to Industry

Our Defense Industrial Base is the target of Foreign Intelligence Entities, who feel they can win the War on our Economy through Industrial Espionage. Since the Defense Department relies on the cleared defense contractors developing our nations' 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 Department of Defense plans in order to exploit its information and impede its mission.

Foreign Intelligence Threats

Traditional FIE Activity includes: Foreign Intelligence Entities operating out of embassies, consulates, universities, and trade missions, internal spies, or their sources: the insider threats.

Non-traditional activity includes foreign government-sponsored commercial enterprises, international trafficking organizations, and terrorist organizations.

What do they Want?

What do they 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.

Intelligence Collection Tradecraft

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

- Intercepts of cell phones, or other wireless signals
- Intercepts of open telephone lines
- Intercepts in hotels while TDY
- Looking through the trash
- Simple conversations, online or in person, and
- Hacking into unclassified or classified systems

Collection and Recruitment Methods

Some methods of operation or “MO” frequently used by foreign intelligence to collect information include:

- Elicitation
- Unsolicited requests for information
- Visits to DoD installations or facilities
- International conventions, seminars, and exhibits
- Solicitation and marketing of services, and
- Cyber Intelligence Gathering

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 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 Visits

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
- 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 pre-approved by security officials 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 servicing CI or security official immediately upon learning that you will be the host of a foreign visit to any government facility or installation. 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 work space.

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 products
- 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, and
- 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, and

- 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.
- U.S. researchers may also receive 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) request 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, 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 in jeopardy the lives of our men and women.

Open Source

Foreign Intelligence Entities also collect information from publicly available sources. Examples of open-source of information include:

- Newspapers,
- Magazines,
- Radio,
- Television, and
- Computer-based information.
- Online communities and user-generated content such as:
    - Social Networking sites,
    - Video sharing site,
    - Wikis, and
    - Blogs
- Government reports, such as:

  - Budgets,
  - Demographics,
  - Hearings,
  - Legislative debates
  - Press conferences, and
  - Speeches 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 5240.06 titled “Counterintelligence Awareness and Reporting (CIAR)” Reportable FIE-Associated cyberspace contacts, activities, indicators, and behaviors include: actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information; password cracking, key logging, steganography, privilege escalation, and account masquerading; network spillage incidents or information compromise; use of DoD account credentials by unauthorized parties; tampering with or introducing unauthorized elements into information systems; unauthorized downloads or uploads of sensitive data; unauthorized use of USB, removable media, or other transfer devices; downloading or installing non-approved computer applications; unauthorized e-mail traffic to foreign destinations; denial of service attacks or suspicious network failures; excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents; any credible anomaly, finding, observation, or indicator associated with other activity behavior that may also be an indicator of terrorism or espionage; data exfiltrated to unauthorized domains, unexplained storage of encrypted data; Hacking or cracking activities; social engineering, electronic elicitation, spoofing, or spear phishing; 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 vs. 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.

The recruitment process is broken down into five phases and may take up to three years to develop. The phases are:

- Spotting;
- Assessing;
- Developing;
- Recruitment; and
- Handling

Spotting Phase

In the Spotting and Assessment 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 Phase

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

Developing Phase

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 Phase

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

Handling Phase

In the Handling Phase 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.

Indicators

Indicators of FIE Targeting

Some indicators of Foreign Intelligence Entities (FIE) targeting are:

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

Potential Espionage Indicators

Potential espionage indicators (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 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, and
- Illegal downloads

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

What is a 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

Detecting 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!

Terrorism and Force Protection

Terrorism

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

Who can forget the December 03, 2015 attack in San Barnardino, 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'd pledged allegiance to ISIS gunned down 49 people in a nightclub in Orlando, Florida - the deadliest mass shooting in the United States and the nation's worst terror attack since 9/11. 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.

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 (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 capture 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.

Responsibilities and Reporting Requirements

So, what should you do? Everyone has CI responsibilities to keep our nations secrets and to protect ourselves and our co-workers. Remember, “if you see something, say something.” To learn more about your CI responsibilities and the Reporting Requirements for CI-related incidents click on the images above.

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’, Provide non-descript answers; leave the talking to someone else Practice good Operations Security! Do not leave sensitive documents or equipment unattended in cars, hotel rooms, or hotel safes. Store the information in appropriate secure facilities like 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/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. A rule of thumb - 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

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's not your job to investigate, but it is your responsibility to report it so authorities can.

Requirements

Everyone is required to report behaviors and indicators of potential FIE threats. DoD personnel should report potential FIE threats 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 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 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

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.