Student Guide

Course: Integrating Counterintelligence (CI) and Threat Awareness into Your Security Program, v2

Lesson: Course Introduction

Contents

Course Information

Purpose	Provide a thorough understanding of how counterintelligence and threat awareness is an essential component of a security program
Audience	Military, civilian, and contractor security professionals and practitioners who develop and maintain security programs
Pass/Fail %	75 percent
Estimated completion time	90 minutes

Course Overview

In the espionage trade, many types of threats exist and many techniques are used to subtly extract information about personnel, their work, and colleagues. Pieces of information collected, classified or not, may be useful to an adversary. By putting small pieces of information from various sources together, adversaries may be able to discover a level of detail that no one source would have been able to provide.

Counterintelligence (CI) and threat awareness are fundamental and critical components for any successful security program. In this course, you will learn about incorporating CI and threat awareness into your program.

Course Objectives

- Identify the purpose of incorporating counterintelligence and threat awareness information into a security program
- Identify counterintelligence and threat awareness policy requirements for Industry and DoD personnel
- Identify the role of the DSS Counterintelligence Directorate
- Identify the role of threat identification in the analytical risk management process
- Identify key types of threats and common methods of operation
- Identify information most likely to be targeted by espionage
- Identify key sources of threat information
- Identify the types of counterintelligence and threat awareness information that should be reported
- Identify counterintelligence and threat information reporting requirements and procedures

Course Structure

- Course Introduction
- Introduction to Counterintelligence and Threat Awareness
- Identifying Threats
- Obtaining Counterintelligence and Threat Information
- Reporting Counterintelligence and Threat Information
- Course Conclusion

Student Guide

Course: Integrating Counterintelligence (CI) and Threat Awareness into Your Security Program, v2

Lesson 2: Introduction to Counterintelligence (CI) and Threat Awareness

Contents

Introduction

Objectives

A security program cannot succeed without counterintelligence (CI) and threat awareness. The cost of failure cannot be measured. This lesson shows why CI and threat awareness are important, and helps identify requirements that must be satisfied.

Lesson objectives are:

- Identify the purpose of incorporating CI and threat awareness information in a security program
- Identify CI and threat awareness policy requirements for Industry and DoD personnel
- Identify the role of the Defense Security Service (DSS) Counterintelligence (CI) Directorate

Why Counterintelligence (CI) and Threat Awareness?

Evolution of Counterintelligence (CI)

Since our country's infancy, the threat of espionage and the damage it could inflict has been real. Government and military leaders have always been concerned with such threats. In the aftermath of World War II, President Truman signed into law the National Security Act of 1947. The act addresses CI and created the National Security Council and the Central Intelligence Agency.

In 1981, President Reagan issued Executive Order 12333, United States Intelligence Activities, which regulates the collection of intelligence information, as well as outlines responsibilities of and cooperation between members of the national intelligence community. Today, EO 12333 continues to shape the practice of CI, which includes—according to the National Counterintelligence Strategy of the U.S.—"defensive and offensive activities conducted at home and abroad to protect against the traditional and emerging foreign intelligence threats of the 21st century.

Over time, as adversaries changed and technological advances grew exponentially, so did the scope of threats from espionage. Today, the types of threats, methods of operation, and their targets cast a wider net than ever. Not only must we remain vigilant for the sake of our national security, but we also must protect trade secrets and the competitive advantage that U.S. companies—and in turn, the U.S. economy—rely on.

As a security official, when you integrate CI and threat awareness into your security program, not only are you protecting the way of life for your country and the lives of its warfighters but you are also protecting your organization, your livelihood, and the livelihood of your co-workers. Just as national security depends on you, so does the ability of U.S. companies to survive and compete in the world economy. Simply put, the U.S. workforce—maybe even *your* employment—depends on *you*.

What is Counterintelligence (CI)?

In order to integrate counterintelligence and threat awareness information into a security program, you need a strong understanding of what counterintelligence is and what it should achieve.

Executive Order 12333 defines counterintelligence as "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents, or international terrorist organizations or activities." Using real-time threat awareness information for countering the threat to classified programs, secrets, technologies, and operations enables the U.S. Government to better protect U.S technology and operations.

This allows the United States to:

- Maintain a strategic advantage
- Assist in force protection
- Provide security awareness tools for establishing security countermeasures
- Ensure the integrity of DoD and U.S. industry program secrets, technologies, and operations
- Protect the lives of our warfighters

Regulatory Basis

Counterintelligence (CI) Requirements

Executive Order 12333 provides the legal requirement to use all reasonable and lawful means to ensure that the United States receives the best intelligence available. CI is part of this requirement. In addition, the EO 12333 requires U.S. intelligence activities to ensure the protection of U.S. persons' rights while employing the least intrusive means when collecting information.

DoD has implemented this requirement in two regulations:

1. DoD 5200.1, Volume 1, Enclosure 3, the DoD Information Security Program, outlines required security education and training as well as procedures for addressing compromised classified information.
2. DoD Directive 5205.16, the Insider Threat Program, includes requirements for continuing security education and reporting requirements.

In addition, DoD Directive 5240.06, Counterintelligence Awareness and Reporting (CIAR), provides further guidance.

Requirements for the intelligence community (IC) are contained in two directives:

1. Intelligence Community Directive (ICD) 700 establishes IC policy for the protection of national intelligence. It provides a framework for greater coordination and communications between counterintelligence and security

activities of the IC to strengthen the ability to identify, deter, disrupt, mitigate, and counteract intelligence activities directed against U.S. interests by foreign powers or activities.

2. ICD 750 establishes the baseline for counterintelligence programs across the IC to create a strategic approach to counterintelligence that will enhance the national security posture of the U.S. The ICD 750 recommends counterintelligence to be functionally integrated with security programs per the ICD 700.

Special requirements for *contractors* are provided in DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM.)

DSS Counterintelligence (CI) Directorate

Role of the DSS Counterintelligence (CI) Directorate

The DSS Counterintelligence (CI) Directorate provides CI support to cleared Defense contractors. This support includes identifying, exploiting, and neutralizing espionage and collection attempts by foreign intelligence and security services.

As a security official, the DSS CI Directorate is a central CI source for you and your organization. If you are a facility security officer (FSO) at a cleared contractor facility, the DSS CI Directorate is one of your primary sources of information. If you are a military member or civilian Government employee, information from this office may supplement what you receive through your chain of command from your designated CI support activity.

The DSS CI Directorate provides early detection and referral of potential espionage cases to applicable CI community and law enforcement entities. The office assists industry in the recognition and reporting of collection attempts by foreign nation state intelligence and non-nation state actors. As part of this role, the office publishes threat information annually and makes it available to cleared contractors. The DSS CI Directorate also helps develop countermeasures and advises industry on their application. Finally, the office supports industry's growing international involvement.

Review Activity 1

Which of the following are goals of integrating CI and threat awareness into a security program? *Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.*

- ☐ Maintain a strategic advantage in operations, programs, and classified research and development
- ☐ Assist in force protection
- ☐ Provide security awareness tools for establishing security countermeasures
- ☐ Ensure integrity of DoD and U.S. industry program secrets, technologies, and operations
- ☐ Protect our warfighters

Review Activity 2

See whether you can remember the purposes of these important policy documents.

Match each document to its matching description. Then check your answers in the Answer Key at the end of this Student Guide.

Documents:

A. DoD 5220.22-M NISPOM
B. E.O. 12333
C. DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR)
D. DoDD 5205.16, Insider Threat Program

Descriptions:

_____ Provides the legal requirement to use lawful means to ensure U.S. receives the best intelligence available

_____ The manual that includes CI-related requirements for industry

_____ Regulation mandating the reporting of suspicious activities or potential espionage indicators

_____ Regulation mandating the establishment of an insider threat program

Lesson Conclusion

Summary

In this lesson, you learned about the purpose and importance of integrating CI and threat awareness into a security program. You also learned about the related policy documents and about the role of the DSS CI Office.

Answer Key

Review Activity 1

- ☑ Maintain a strategic advantage in operations, programs, and classified research and development (correct answer)
- ☑ Assist in force protection (correct answer)
- ☑ Provide security awareness tools for establishing security countermeasures (correct answer)
- ☑ Ensure integrity of DoD and U.S. industry program secrets, technologies, and operations (correct answer)
- ☑ Protect our warfighters (correct answer)

Review Activity 2

Documents:

A. DoD 5220.22-M NISPOM
B. E.O. 12333
C. DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR)
D. DoDD 5205.16, Insider Threat Program

Descriptions:

B	Provides the legal requirement to use lawful means to ensure U.S. receives the best intelligence available
A	The manual that includes CI-related requirements for industry
C	Regulation mandating the reporting of suspicious activities or potential espionage indicators
D	Regulation mandating the establishment of an insider threat program

Student Guide

Course: Integrating Counterintelligence (CI) and Threat Awareness into Your Security Program, v2

Lesson 3: Identifying Threats

Contents

Introduction

Objectives

Threats can come from anywhere, and they may present themselves in various ways, targeting various types of information or systems.

As a security official, it is your duty to understand the threats you encounter. The success of your security program depends on your ability to identify what must be protected and what—or who—might threaten it.

Lesson objectives are:

- Identify the role of threat identification in the analytical risk management process
- Identify key types of threats and common methods of operation used for collecting information
- Identify information most likely to be targeted by espionage

Analytical Risk Management Process

Opening

You may be familiar with Chi Mak. As an electrical engineer for a Defense contractor, Chi Mak worked on more than 200 U.S. Defense and military contracts over a 20-year span. In 2008, Mak was eventually convicted for acting as an unregistered foreign agent of China and sentenced to 24 and 1/2 years in prison for conspiring to export technology related to Navy ships. As a security official, do you have the systems in place that will prevent a spy from entering your facility?

Applying Risk Management

How well do you understand your organization's assets and how they may be compromised? Do you understand the threats your organization faces, its vulnerabilities, and the associated risks? What types of countermeasures do you have in place to mitigate these risks?

Risk Management Steps:

Step 1: Identify Assets

Step 2: Identify Threats

Step 3: Identify Vulnerabilities

Step 4: Assess Risk

Step 5: Develop and Apply Countermeasures

Understanding and applying risk management is fundamental to incorporating CI and threat awareness into your security program. Knowing what each step means to your organization could prevent a spy or other threat from succeeding within your organization. This course focuses on the steps for identifying assets and threats, but it is important to understand how each of the steps fit into the overall Risk Management model.

a. Identify Assets

To protect against threats, you must first understand what requires protection. That is, what are your organization's assets? Think about the information or items in your organization. What may be a potential target? You must adopt the mindset of a spy—what is valuable? Don't simply think in terms of classified systems and information. Assets can include both classified and sensitive information.

This course focuses on *information* as the type of asset that we are protecting. When applied more generally, analytical risk management considers *all* assets; information, as well as buildings, equipment, material, supplies, and people. Operations Security (OPSEC) applies this five-step model to the process of protecting *unclassified* critical information.

In this course we consider both classified and unclassified information as assets we want to protect.

b. Identify Threats

Next, identify the threats you face. Can you identify your adversaries? Who are the adversaries of your company or organization? Who are the adversaries of the Government program you support? Who wants to gain unauthorized access to information you protect? Do you know the capabilities and intentions of these adversaries?

The ability to identify threats is an essential component of a successful security program.

c. Identify Vulnerabilities

You must also be able to identify the chinks in your organization's armor. What types of weaknesses exist that create vulnerabilities? Are there weaknesses in information systems? In policies and procedures? Or in the implementation of security practices?

You must understand these vulnerabilities and consider how an adversary may exploit them.

d. Assess Risk

Now think about the impact of your assets being compromised. What is the worst that could happen? Loss of economic, market, and competitive advantage? Loss of strategic and military advantage? Loss of jobs? Or loss of life?

When you consider and calculate overall risk, you must consider threats, vulnerabilities, and their impacts.

e. Develop and Apply Countermeasures

Finally, once you have considered your assets and the potential impact of compromise of those assets, your sources of threat, your vulnerabilities, and the risks associated with each, you need to think about what countermeasures you can develop and apply to mitigate these concerns.

The success of your security program depends on your ability to develop and apply such countermeasures. In addition, regulations provide standards for security measures to protect classified information.

When you consider countermeasures, you must also consider which measures are needed to protect export controlled and other sensitive unclassified information.

Assets

Opening

In espionage cases, the cornerstone of the defense is often that the defendant was unaware that the stolen information was classified, export-controlled, or proprietary.

If it cannot be shown that reasonable measures were taken to clearly identify classified, proprietary, or other sensitive information and ensure its protection, an espionage case may be dismissed.

As a security official, the success of your security program relies on your ability to identify what must be protected. In the event that someone is successful at obtaining and misusing information, the ability to bring that person to justice relies on how well you previously identified vulnerabilities and threats to your assets and implemented measures to protect the information.

Identifying Assets

Adversaries are interested in *anything* that may be used to weaken U.S. advantage—whether it is a military, competitive, or economic advantage. As a security official, your job is to ensure that your organization protects against these adversaries.

What, specifically, should be protected? While the specific information and resources will vary across organizations, you must protect any information, technology, or system that, if compromised, would:

- Significantly damage national security
- Alter program direction
- Compromise the program or system capabilities
- Shorten the expected life of the system
- Require research, development, testing, and evaluation to counter the loss's impact

a. Assets

When identifying assets, how do you know what should be included? Some valuable assets have already been identified for you. For example, any information that is subject to export controls must be protected.

Other examples of information that requires protection include proprietary, personal, and critical program information. Classified information has been identified as a valuable asset. The level of classification for each item of information is determined by the impact that would be caused by unauthorized disclosure.

You can also identify assets by working with others within your organization. Program managers, company officials, engineers, and scientists generally have the most knowledge about the sensitivity and value of assets.

As a security official, understanding the nature and value of the assets being protected will allow you to make decisions about related vulnerabilities and security countermeasures. It also helps ensure that critical assets will be protected *first* and that resources will be allocated where they will be most effective.

1. Targeted Technologies

Technology assets are the greatest target of our adversaries. Both classified and unclassified technologies are targeted.

A major target is technology that would allow significant advances in the development, production, and use of military capabilities of potential adversaries. This is referred to as *militarily critical technology*. DoD maintains a list of this technology. Not surprisingly, its export is strictly controlled by the International Traffic in Arms Regulations (ITAR).

Technology that has both military and commercial use—or *dual use* technology— is also a major target. Among other things, dual use technology may be used to develop weapons and weapons of mass destruction or other military equipment. As such, its export is strictly controlled and enforced under the Export Administration Regulations.

As a security official, you must understand the technologies within your organization that may be targeted and you also must be aware of the regulations that govern their export.

a. International Traffic in Arms Regulations

ITAR implements the provisions of the Arms Export Control Act (AECA) and controls export and import of Defense-related articles and services on the U.S. Munitions List.

The Department of State enforces the ITAR regulations. They dictate that information and material pertaining to Defense- and military-related technologies may not be shared with foreign persons without authorization from the Department of State or a special exemption.

The list of ITAR-controlled Defense articles, services, and technology changes. As a security official, it is important you keep up to date on items that apply to your facility.

b. Export Administration Regulations

The Bureau of Industry and Security (BIS) of the Department of Commerce is responsible for licensing products that are "dual-use," or have both commercial and military or proliferation applications.

Export Administration Regulations (EAR) deal with dual-use technologies and are enforced by the Department of Commerce. EAR-controlled items are those that can be used both in military and other strategic uses and in commercial applications.

The EAR restricts access to dual use items by countries or persons that might apply such items to uses against U.S. interests. These include controls designed to stem the proliferation of weapons of mass destruction and controls designed to limit the military capability of certain countries, and stop the support of terrorism. The EAR also protects the United States from the adverse impact of the unrestricted export of commodities in short supply.

As a security official, you must identify items within your facility that fall under EAR. You can do so by referencing the Export Administration Database.

2. Information Known by Personnel

When you consider which assets within your organization must be protected, remember that *you* and your *coworkers* are potential targets.

Knowledge of your organization is extremely valuable to an adversary. What are the key questions adversary officials are likely to ask about *our* intentions, capabilities, and activities? You must consider these questions. Our adversaries do. And they use them to obtain answers critical to *their* operational effectiveness.

Think about what you and other personnel know about the status of technology development. What damage would this information do in the wrong hands? How long would it take for your organization to undo such damage? Could the damage be

undone? Adversaries also find information regarding the personalities of key leaders valuable; as such information could provide them additional clues to gaining even more information. Not surprisingly, adversaries are always interested in learning about a program's milestones and specifications, the issues and solutions associated with the program, and an organization's special projects and programs.

Each item of information is like a piece of a puzzle. If our adversaries collect enough pieces of the puzzle, they will be able to use this knowledge against us.

Threat Types and Collection Methods

1. Threat Types

Do you know what a threat looks like? Can you say with certainty that you could spot one if confronted?

Some threats are found within your office and look just like you and your coworkers. In fact, they may *be* your coworkers. Others originate thousands of miles and an ocean away within foreign intelligence agencies. Yet others are tangled in illegal activities, shrouding themselves under the cover of other activity. Still others are found in the business section of your local newspaper.

To identify these threats, you must understand *what* or *who* to look for, and you must understand *how* they operate.

Threat types include:

- Insider threats
- Threats from foreign intelligence service
- Terrorist organizations
- Criminal activities
- Business competitors

2. Information Collection Methods

There are five general categories of information collection methodologies.

- Human Intelligence uses people to gather information.
- Signals Intelligence involves the collection of electronic signals, including phone calls and e-mails.
- Imagery Intelligence uses satellite imagery, photographs, and other images to collect information.
- Open Source Intelligence gathers information that is legally and publically available, including information from the news media and Internet.
- Measures and Signatures Intelligence is technically derived intelligence that uses the unique characteristics of fixed and dynamic target sources.

Most of the examples found in the rest of this lesson are in the general category of human intelligence, but keep in mind that an adversary is likely to use a variety of collection methods in an attempt to obtain the information that you are trying to protect.

3. Methods of Operation

Threats come in various forms, and use a variety of methods to gain information.

Understanding their methods can help you identify the presence of a threat. Consolidated information about each of these methodologies may be found in the Counterintelligence Best Practices for Cleared Industry booklet, distributed by the DSS CI Directorate.

Collection methods:

- Unsolicited requests
- Joint ventures and research
- Cyber threats
- Visits to facilities
- Conferences, conventions, and trade shows
- Targeting insiders

4. Unsolicited Requests

Case Study Example

A cleared U.S. company received a request to market a software program with intelligence applications to an Eastern European security organization. The sensitive nature of the software's capabilities makes it an export-controlled technology. Because the software is an export-controlled technology, the U.S. company knew it could not sell it to a foreign organization.

Would personnel at your facility recognize such a request as a threat?

An unsolicited request for information is one that was not sought or encouraged. Those types of requests may come from a known or unknown company or individual, or from another country. Unsolicited requests are the most frequently reported method of operation associated with foreign collection activity. Requests frequently involve e-mailing, phoning, or mailing directly to individual U.S. individuals rather than to corporate marketing departments.

There are several indicators that can help you and your employees identify suspicious requests and several recommended countermeasures you can employ.

a. Indicators

The following are potential indicators of unsolicited requests. The sender:

- Has a foreign address
- Has never met recipient
- Identifies self as a student or consultant
- Identifies employer as a foreign government
- States that work is being done for a foreign government or program
- Asks about a technology related to a Defense program, project, or contract
- Asks questions about Defense-related programs using acronyms specific to the program
- Insinuates the third party he/she works for is "classified" or otherwise sensitive
- Admits he/she could not get the information elsewhere because it was classified or controlled
- Advises recipient to disregard the request if it causes a security problem, or the request is for information the recipient cannot provide because of limitations such as security classification or export controls
- Advises recipient not to worry about security concerns
- Assures recipient that export licenses are not required or not a problem

b. Countermeasures

The following countermeasures can protect against unsolicited requests:

- View unsolicited requests with suspicion, especially those received on the Internet
- Respond only to people who are known after verifying their identity and address
- If the requester cannot be verified:

  - Do not respond in any way
  - Report the incident to security personnel

5. Visits to Facilities

Case Study Example

During a visit to an aeronautics facility, a foreign delegation of 10 people was provided with 1 escort. The visiting delegation recognized the vulnerability and used an opportunity during a break to separate, causing half the delegation to be unescorted in an area with export-controlled technology.

What security measures does your facility have in place designed to protect itself from potential wayward visitors?

As a necessary part of doing business, your organization likely hosts visitors at your facility. While *any* visitor may pose a security threat, of specific concern are *foreign*

visitors. While not every visitor seeks to do you harm—and in fact, the vast majority do not—as a security official, it is your responsibility to ensure that policies are in place that will protect against wayward visitors.

While not the most frequently used collection method, it may be one of the most damaging collection activities as it can result in the loss of technology. A suspicious contact can occur before, during, or after a visit and may come from one-time visitors; long-term visitors, such as exchange employees, official government representatives, or students; and frequent visitors, such as sales representatives and business associates.

There are many indicators of suspicious conduct related to visits and countermeasures you can employ to protect your facility.

a. Indicators

Suspicious or inappropriate conduct during visits can include:

- Requests for information outside the scope of what was approved for discussion
- Hidden agendas associated with the stated purpose of the visit
- Visitors/students requesting information and becoming irate upon denial
- Individuals bringing cameras and/or video equipment into areas where no photographs are allowed

b. Countermeasures

The following countermeasures can protect against unauthorized access by foreign visitors:

- Contractors may coordinate with DSS prior to visit
- Prior to visit, brief hosts and escorts on approved procedures
- Walk visitor route and identify vulnerabilities
- Prior to the visit, notify all employees about the visit, restrictions on the visitors and the nature of the threat
- Debrief personnel in contact with visitors
- Ensure visitors do not bring recording devices, including cell phones, into the facility
- Develop a Technology Control Plan (TCP), that:
  - Stipulates how a company will control access to its export-controlled technology
  - Outlines the specific information authorized for release
  - May be required by the National Industrial Security Program Operating Manual (NISPOM) and the International Traffic in Arms Regulations (ITAR) under certain circumstances
  - Protects:
    - Classified and export-controlled information
    - Control access by foreign visitors
    - Control access by employees who are foreign persons

6. Joint Ventures and Research

Case Study Example

An engineering team from a U.S. Defense contractor participated in an approved exchange with a foreign counterpart team during which approved unclassified technical information was commonly shared among participants.

Following the exchange program's completion, representatives of the U.S. company discovered several export-restricted documents among material left on-site by the foreign team.

Clearly, the foreign team had an agenda beyond the scope of the U.S. Defense contractor's expectations. Would personnel at your facility recognize such a request as a threat?

Joint ventures and research and development partnerships provide significant collection opportunities for foreign interests. Such business or academic relationships often place foreign entities alongside U.S. personnel and technology, thus facilitating access to protected programs. There are many indicators of this collection practice and countermeasures you can put in place.

a. Indicators

During joint ventures:

- Foreign visitors mail or fax documents written in a foreign language to a foreign embassy or foreign country
- Foreign visitors request for:
    - Access to a local area network (LAN)
    - Unrestricted facility access
    - Company personnel information

During the bidding process: Personnel request detailed technical data, then cancel contract.

b. Countermeasures

The following countermeasures may guard against threats that may come from joint ventures and research:

- Review all documents being faxed or mailed; use a translator, when necessary
- Provide foreign representatives with stand-alone computers
- Share the minimum amount of information appropriate to the scope of the joint venture/research
- Educate employees extensively

- Project scope
- Handling and reporting elicitation
- Sustainment training

- Refuse to accept unnecessary foreign representatives into the facility
- Develop a TCP

7. Conferences, Conventions, and Trade Shows

Case Study Example

A lead engineer for a U.S. Defense contractor received an all-expenses-paid invitation to lecture in the Far East. The engineer accepted, and once there, noticed several people recording her lecture. After the lecture, the engineer became uncomfortable with the large number of questions around classified aspects of her work.

Would personnel at your facility view such events as a potential threat?

Conferences, conventions, and trade shows directly link programs and technologies with knowledgeable personnel. Personnel may be invited to share their knowledge at such forums. Once at the forum, they may be pressed for restricted, proprietary, or classified information.

They may also be targeted while traveling to or from the event. Personnel must be aware that telephone monitoring and hotel room intrusions are a possibility. They may also be singled out by foreign customs where their computers, cell phone, and PDA may be targeted.

There are several indicators you can use to help employees identify when they may be a target, and there are several countermeasures you can put in place to guard against this technique.

a. Indicators

The following are suspicious indicators related to conferences, conventions, and trade shows:

Prior to event:

- Personnel receive an all-expenses-paid invitation to lecture in a foreign nation
- Host unsuccessfully attempted to visit facilities in the past
- Entities want a summary of the requested presentation or brief 6 to 12 months before lecture date

During event:

- Conversations involving classified, sensitive, or export-controlled technologies or products
- 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
- Attendees wear false name tags

b. Countermeasures

The following countermeasures can be taken to guard against threats that may come from seminars, conventions, and exhibits:

- Consider what information is being exposed, where, when, and to whom
- Provide employees with detailed travel briefings concerning:
    - The threat
    - Precautions to take
    - How to react to elicitation
- Take mock-up displays instead of real equipment
- Request a threat assessment from the program office
- Restrict information provided to only what is necessary for travel and hotel accommodations
- Carefully consider whether equipment or software can be adequately protected

8. Solicitation and Marketing of Services

Case Study Example

A foreign student studying aerodynamics at a major foreign university contacted a U.S. Defense company about the possibility of an intern position in the company's aerodynamics research branch. The student expressed specific interest in working on research related to classified and export restricted technology known to be actively sought by the student's country of origin.

Could a request like this be a threat?

Adversaries may attempt to gain employment with cleared companies in unclassified positions. This is most often associated with foreign adversaries, though business competitors may also use this technique. Scientists and engineers will offer their services to research facilities, academic institutions, and cleared Defense contractors.

This offer may be a means to place an adversary inside the facility to collect information on a desired technology.

There are several suspicious indicators related to the solicitation and marketing of services and there are several countermeasures you can put in place to guard against this technique.

a. Indicators

The following are suspicious indicators related to the solicitation and marketing of services:

- Invitations for:
  - Cultural exchanges
  - Individual-to-individual exchanges
  - 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
  - U.S. personnel assigned overseas are most targeted by this method
  - Be aware that listening devices may be implanted in equipment
- Outsourcing software/program writing
  - Be aware that outsourcing provides opportunity for sensitive data to be improperly used or sold by foreigners
  - Be aware that malware, viruses, or malicious code may be intentionally implanted into system

b. Countermeasures

The following countermeasures can be taken to guard against this collection method:

- Provide employees with periodic security awareness briefings with regard to long-term foreign visitors
- Check backgrounds and references
- Request a threat assessment from the program office or your CI support activity
- Require that participants sign a legally enforceable non-disclosure agreement
- Limit dissemination of sensitive information based on a need-to-know principle
- Develop and implement a TCP

9. Cyber Threat

Case Study Example

A U.S. Defense company received multiple deceptive e-mails that, when opened, resulted in malicious software being automatically installed on the company's internal computer system.

Would personnel at your facility recognize this as a possible *targeted* intrusion seeking specific information or would they assume it was only a random attack?

Not surprisingly, the Internet is the fastest growing method of operation for adversaries.

Use of the Internet offers a variety of advantages to our adversaries; it is simple, low cost, nonthreatening, and relatively risk-free for anyone attempting to collect classified, proprietary, or sensitive information. Adversaries may use this method to input corrupt data, send viruses, or hack into an organization’s system. They may also use the Internet to solicit personnel via chat rooms or e-mail.

A wide variety of knowledgeable persons can be contacted and information may be collected from each based on that person’s area of expertise. When the information is put together, a level of detail is often revealed that no one individual would have been able to provide. While any type of adversary may use this method, it is the most frequently used method of foreign countries.

There are several indicators you can use to help personnel identify when they may be a target and there are countermeasures you can employ to protect against this type of threat.

a. Indicators

The following is a list of suspicious indicators related to cyber threats:

- Unauthorized system access attempts
- Unauthorized system access to or disclosure of information
- Any acts that interrupt or result in a denial of service
- Unauthorized data storage or transmission
- Unauthorized hardware and software modifications
- E-mails received from unknown senders with foreign addresses

b. Countermeasures

The following countermeasures can be taken to guard against cyber threats:

- Develop and implement a TCP
- Conduct frequent computer audits

- Ideally: Daily
- At minimum: Weekly

- Do not rely upon firewalls to protect against all attacks
- Report intrusion attempts
- Direct personnel to avoid responding to any unknown request and to report these requests
- Disconnect computer system temporarily in the event of a severe attack
- Don't open attachments from suspicious emails

10. Targeting Insiders

Case Study Example

Many Americans, and certainly those in the security field, know the name Aldrich Ames.

Mr. Ames is a former CIA counterintelligence agent and analyst. In 1994, he was convicted of spying for the former Soviet Union and Russia.

Does your facility have procedures in place that will help recognize and stop a threat from within?

Adversaries may target insiders in different ways. Unknowing and unwilling personnel may be targeted to provide information using any of the methods previously discussed or adversaries may use these methods to target personnel to become willing spies.

Because insiders have much knowledge of and access to their organization's resources, the potential for damage is boundless. Threats from insiders can be very difficult to ascertain. Insiders look like you and me because they *are* you and me: an employee, a contractor . . . *anyone* who has legitimate access to an organization.

There are several indicators you can use to help identify potential espionage among insiders, and there are countermeasures you can employ to protect against the threat from insiders.

a. Potential Espionage Indicators

The following is a list of potential espionage indicators:

- Alcohol or other substance abuse or dependence
- Mental health issues
- Extreme, persistent interpersonal difficulties
- Hostile or vindictive behavior
- Criminal behavior
- Financial difficulties
- Unexplained or sudden affluence
- Unreported foreign contact and travel
- Inappropriate, unusual, or excessive interest in classified information

- Misuse of computers
- Divided loyalty or allegiance to the United States
- Works hours inconsistent with job assignment
- Repeated security violations
- Reluctance to take polygraph

b. Countermeasures

The following countermeasures can be taken to guard against the insider threat:

- Provide training on the insider threat
- Brief employees on elicitation methods
- Brief employees to be alert to actions of other employees
- Monitor the activities of foreign visitors for indications that they are targeting company personnel
- Require that personnel sign a legally enforceable non-disclosure agreement
- Limit dissemination of sensitive information based on need-to-know basis

Review Activity 1

You are working with your organization's senior leaders to identify the organization's assets. Which of the following are characteristics of information, technology, or systems that should be protected? Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

Protect anything that, if compromised, would:

- ☐ Significantly damage national security
- ☐ Alter the program's direction
- ☐ Compromise the program or system capabilities
- ☐ Shorten the expected system life
- ☐ Require research and development to counter the impact of loss

Review Activity 2

Your company receives a request seeking export-restricted products from the procurement department of a foreign company. How should your organization respond? Select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.

- ○ Times are tough and business is business. Turning any customer away is foolish; accept the sale and find a way to avoid compliance with the export restrictions.
- ○ You cannot directly sell the product to the foreign organization, but the marketing department may be able to find a way to get it to them.
- ○ Export control laws are in place for a reason. Prior to disclosing any information, obtain an export authorization (such as an export license) from the U.S. Government.

Review Activity 3

You know that the presence of certain life experiences can make a person more likely to commit espionage than someone who does not have such experiences. Based on potential espionage indicators, which of the following would be most likely to commit espionage? Select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.

- ○ Bob: Little league baseball coach, married father of four, $380,000 mortgage
- ○ John: Regularly drinks excessively, recently divorced, paid cash for $635,000 home
- ○ Maria: Has family in Mexico, single with no children, rents a modest apartment
- ○ Saul: Avid poker player, divorced 20 years with two grown children, lives with elderly mother

Review Activity 4

Match each collection method to its matching description.

Then check your answers in the Answer Key at the end of this Student Guide.

Collection Methods:

A. Unsolicited Request
B. Cyber Threat
C. Conferences, Conventions, and Trade Shows
D. Joint Ventures and Research
E. Solicitation of Marking and Services
F. Targeting Insiders

Descriptions:

_____ Technical experts may receive invitations to share their knowledge

_____ Is the fastest growing method of operation for adversaries

_____ Provide an opportunity to build relationships

_____ When successful, places adversary inside facility to collect information on desired technology

_____ May be received from a foreign address and from someone the receiver has never met

_____ Has the potential to inflict the greatest amount of damage over any other type of collection method

Lesson Conclusion

1. Summary

In this lesson, you were introduced to the analytical risk management process, and learned specifically about its first two steps—Identifying Assets and Identifying Threats. You learned about identifying assets and targeted information. You learned about threat types and how to recognize threats by the collection methods they may use.

Answer Key

Review Activity 1

Protect anything that, if compromised, would:

- ☑ Significantly damage national security (correct answer)
- ☑ Alter the program's direction (correct answer)
- ☑ Compromise the program or system capabilities (correct answer)
- ☑ Shorten the expected system life (correct answer)
- ☑ Require research and development to counter the impact of loss (correct answer)

Review Activity 2

- ○ Times are tough and business is business. Turning any customer away is foolish; accept the sale and find a way to avoid compliance with the export restrictions.
- ○ You cannot directly sell the product to the foreign organization, but the marketing department may be able to find a way to get it to them.
- ● Export control laws are in place for a reason. Prior to disclosing any information, obtain an export authorization (such as an export license) from the U.S. Government. (correct answer)

Review Activity 3

- ○ Bob: Little league baseball coach, married father of four, $380,000 mortgage
- ● John: Regularly drinks excessively, recently divorced, paid cash for $635,000 home (correct answer)
- ○ Maria: Has family in Mexico, single with no children, rents a modest apartment
- ○ Saul: Avid poker player, divorced 20 years with two grown children, lives with elderly mother

Review Activity 4

Collection Methods:

A. Unsolicited Request
B. Cyber Threat
C. Conferences, Conventions, and Trade Shows
D. Joint Ventures and Research
E. Solicitation of Marking and Services
F. Targeting Insiders

Descriptions:

C	Technical experts may receive invitations to share their knowledge
B	Is the fastest growing method of operation for adversaries
D	Provide an opportunity to build relationships
E	When successful, places adversary inside facility to collect information on desired technology
A	May be received from a foreign address and from someone the receiver has never met
F	Has the potential to inflict the greatest amount of damage over any other type of collection method

Student Guide

Course: Integrating Counterintelligence (CI) and Threat Awareness into Your Security Program, v2

Lesson 4: Obtaining Counterintelligence (CI) and Threat Information

Contents

Introduction

Objectives

As a security official, you must know about current threats so you can integrate counterintelligence and threat awareness into your security program. This lesson shows you where you can turn to find threat information.

Here is the lesson objective.

- Identify key sources of threat information

Why Seek Out Information?

Opening

Bob is a security official at his facility. He is charged with ensuring that his facility's security program can adequately protect and defend against the threat of espionage. Recently, there were several strange occurrences within the facility—unexplained network outages, key files missing, a few employees suddenly working odd hours with no apparent explanation, and the surprise arrival of unexpected foreign visitors.

Bob doesn't think anything of this, but he *should*. If he were paying attention, he'd suspect that someone is targeting his firm. He'd know that similar events have been happening at other facilities like his. If Bob knew about his adversaries and what they had done at other facilities such as his own, perhaps Bob would see that his facility is at risk.

So *how* would Bob know these things? What can Bob *do* to learn about the activities or situations that may threaten him? The information is readily available, and available for Bob to use to discern how his facility could be targeted. Bob needs to pay attention and use the information available to him.

Sources of Information

Information about potential threats is all around you. It is up to you to seek it out and learn from it. Threat summaries and intelligence reports can provide an overall picture of the threat, though this picture must be tailored to your specific facility.

Who might be interested in the classified and unclassified critical information that you need to protect?

Why they would be interested—that is, why they would need the information?

How they might go about collecting it?

Tailoring the threat picture involves examining both national and local intelligence sources as well as government and public sources. There is information available to you from various government agencies and there is open source information all around you.

Let's first take a look at information available to you from government agencies.

Government and Agency Sources

Available Sources

Government and agency sources of threat information include your own organization's counterintelligence (CI) support activity.

Contractors may request threat information from:

- Their Government contracting activity (GCA)
- The DSS Counterintelligence (CI) Directorate
- The Federal Bureau of Investigation (FBI)
- Other Federal, State, and local agencies

Security officers in a military or DoD organization should go through their chain of command and use their organization's CI activity as the primary source of information.

Each of those sources can provide valuable threat information. But it is up to you to seek it out.

Government Contracting Activity (GCA)

If you are a contractor, your Government contracting activity may be the logical first step in obtaining threat information. Individuals there—such as the contracting officer (COTR), security officer, or CI special agent—may be able to provide you with contract-specific threat information; that is, what specifically does your facility *have* or *do* that may make it a target?

A GCA may also be able to provide you with program threat assessments. Such assessments will help you determine the areas of your facility requiring the greatest protection and what to guard against and look out for.

DSS Counterintelligence Directorate

The DSS CI Directorate publishes a trend report every year. It summarizes the threat reports received from cleared contractor facilities and provides information showing trends related to *what* is targeted and the methods used. These publications identify adversaries reported by cleared contractors as suspected collectors of critical technologies being developed at their facilities.

You must familiarize yourself with this report and consider how its information affects you: Where does your facility fall within the types of targeted technologies? What can it tell you about how you may be approached and who may approach you?

Although the report is based on incidents at contractor facilities it is also relevant to military units, DoD Agencies, and other U.S. Government agencies. Classified editions

of these reports, which contain more detailed information, are available from the DSS CI Directorate to security professionals with appropriate clearance and need-to-know.

FBI

The FBI has primary responsibility for counterintelligence investigations within the United States. They also strive to prevent espionage. As part of this responsibility, the FBI partners with other Government entities, academic institutions, and the private sector to share and exchange information. This exchange of information is essential to protecting the national and economic security of the United States.

As a security official, you should use these FBI resources that provide threat information related to espionage, counterintelligence, counterterrorism, economic espionage, cyber and physical infrastructure protection, and all national security issues.

The CI Strategic Partnership is a program that shares information related to our vulnerability to foreign powers, terrorist groups, and other criminal elements. In addition, InfraGard provides information related mainly to cyber threats and threats to critical infrastructure.

You should contact your local FBI office to become involved in these programs and to request more specific threat information when needed.

DoD and Military Counterintelligence (CI) Activities

If you are a military member or civilian security specialist supporting a military command, unit, or organization, you should coordinate through your chain of command to use your organization's designated CI support activity as your primary source of threat information.

Sources include:

- U.S. Army Intelligence Command (INSCOM)
- U.S. Air Force Office of Special Investigations (OSI)
- Naval Criminal Investigative Service (NCIS)
- Defense Criminal Investigative Service (DCIS)

Other Federal, State, and Local Agencies

You can find threat information from a variety of other Government sources.

Here are some other valuable Federal sources you may wish to consult, though keep in mind that this is not an exhaustive list. As a security official, you must seek out information from whatever sources are appropriate based on your facility's capabilities and the threats you may face:

- Department of Homeland Security (DHS)
- Defense Intelligence Agency (DIA)
- Department of State Bureau of Diplomatic Security

- National Counterintelligence and Security Center (NCSC)
- The Office of the National Counterintelligence Executive (ONCIX)
- The Interagency OPSEC Support Staff

Open Sources

Where to Seek Information

Open sources of threat information are all around you. You must seek this information and use it to determine how your facility may be targeted and threatened.

Open sources include:

- News media
- Books
- Internet
- Government publications and Web sites
- Publications of foreign governments
- Publications of other companies

Based on the security needs of your facility, you should seek out threat information from whatever sources are available.

Review Activities

As you know, strange things have been happening at Bob's facility, including:

- Unexplained network outages
- Key files missing
- Employees working odd hours
- Unexpected foreign visitors

Now that you know where Bob can look for threat information, see if you can determine the best solution for the following situations.

Review Activity 1

How should Bob and other security officials expect to receive threat information? Select the correct response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Information on threats will be provided by the appropriate authorities, as needed.
- ○ Bob and all security officials must be proactive and seek out threat information.

Review Activity 2

Bob needs to gather threat information. What sources can he turn to? Select the correct responses. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Newspapers
- ☐ Books
- ☐ FBI
- ☐ GCA
- ☐ Internet
- ☐ DSS CI Directorate
- ☐ Local law enforcement
- ☐ State and Federal agencies

Lesson Conclusion

Summary

In this lesson, you learned that it is your responsibility to seek threat information.

You learned about Government and agency sources as well as some good open sources of this information.

Answer Key

Review Activity 1

Bob and all security officials must be proactive and seek out threat information. (correct answer)

Review Activity 2

- ☑ Newspapers (correct answer)
- ☑ Books (correct answer)
- ☑ FBI (correct answer)
- ☑ GCA (correct answer)
- ☑ Internet (correct answer)
- ☑ DSS CI Directorate (correct answer)
- ☑ Local law enforcement (correct answer)
- ☑ State and Federal agencies (correct answer)

Student Guide

Course: Integrating Counterintelligence (CI) and Threat Awareness into Your Security Program, v2

Lesson 5: Reporting Counterintelligence (CI) and Threat Information

Contents

Introduction

Objectives

As a security official, it is essential that you report incidents and behaviors that may threaten your facility. It will help protect you, and will also educate others about the dangers they face. This lesson shows you what you must report and the requirements for doing so.

Here are the lesson objectives.

- Identify the types of counterintelligence (CI) and threat awareness information that should be reported
    - Suspicious contacts
    - Espionage, sabotage, terrorism, or subversive activities
- Identify CI and threat information reporting requirements and procedures

Why Report?

Opening

Remember the strange things that have been happening at Bob's facility?

Recent events at Bob's facility:

- Unexplained network outages
- Key files missing
- Employees working odd hours
- Unexpected foreign visitors

Bob is unaware that across the country, Sally, a security official at another facility, has also been experiencing issues. Recently, several employees have been approached about providing information about the facility's new, export-controlled technology.

Bob also does not know about James, who is a security official at a facility in the Midwest. His facility's internal file-sharing network was recently hacked.

And then there's John, who works in yet another facility. At his facility, personnel discovered that a highly restricted area was compromised, though it's unclear if anything was taken.

Bob, Sally, James, and John do not know one another. They are not familiar with each other's facilities. Each of them may be unaware that others are experiencing strange events; yet, in some instances seemingly unrelated events at different locations may actually be part of a pattern of foreign collection activity.

If Bob, Sally, James, and John all report these events—as they should and are required to do—a larger picture may emerge and unveil a larger, coordinated threat. However, if any one of them fails to report their facility's event, the threat picture is incomplete. The missing piece of information may be the link to realizing the larger threat that looms.

So how do you know *what* to report? And how do you know *how* it should be reported?

Let's take a look.

Reporting Requirements

Contractor and DoD Requirements

The first line of defense against espionage is your personnel. As such, it is essential they report any incident or behavior that may be related to a potential compromise of classified information or inappropriate disclosure of sensitive unclassified information.

DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM) and DoD Directive 5240.06, CI Awareness and Reporting (CIAR), outline reporting requirements for contractors and DoD personnel.

NISPOM states that contractors are required to report certain events that:

- Impact on the status of the facility clearance
- Impact the status of an employee's personnel security clearance
- Affect proper safeguarding of classified information
- Indicate classified information was lost or compromised

More specifically, contractors are required to report security violations and any suspicious contacts. They are also required to report information concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities.

DoDD 5240.06 requires that DoD personnel report information concerning security violations and other information with potentially serious security significance regarding someone with access to classified information or who is employed in a sensitive position.

Reportable Events and Behaviors

Overview

The NISPOM and DoDD 5240.06 list several reportable events and behaviors that can be categorized broadly in four ways.

1. You must report events or behaviors related to ***recruitment***. That is, you must report any evidence of personnel suspected of being targeted to commit espionage as well as any evidence of personnel volunteering for or soliciting recruitment.
2. Any evidence of ***information collection***—whether it is by way of physically stealing information, hacking into a network, or by other means—must also be reported.

3. In addition, events related to ***information transmittal*** must also be reported. Any events or behaviors that indicate classified, sensitive, or protected information is suspected of being improperly passed or shared with an unauthorized person or entity must be reported.
4. Finally, in addition to behaviors and events around recruitment and information collection and transmittal, ***suspicious behaviors*** must also be reported.

Recruitment

Consider this scenario: Maria is an engineer for a U.S. Defense contractor. She recently participated in an approved exchange with a foreign firm. Upon returning from her exchange, her coworkers notice she received several phone calls from individuals from the foreign firm. In addition, it is later revealed that Maria has been offered a large loan from the foreign firm. Should these events be reported?

Foreign intelligence entities are on the lookout for people who can be solicited to commit espionage against the United States. At the same time, willing would-be spies may volunteer for recruitment by approaching foreign intelligence operatives on their own. Intercepting these relationships is a major task of CI.

Recruitment starts with an initial contact between the foreign intelligence agency and the potential spy, whether by direct recruitment or by volunteering. While the recruitment relationship almost always involves contacts with foreigners, an already committed U.S. spy may approach personnel on the job for recruitment into espionage.

When you consider events or incidents that may be related to recruitment, you must keep in mind that signs of recruitment do not necessarily involve foreigners. Take a moment to review the incidents listed here that must be reported. Keep in mind this is not a complete list. When in doubt, always err on the side of caution. If there is any question of whether an event or behavior should be reported, report it.

Report:

- Contact with an individual associated with a foreign intelligence, security, or terrorist organization
- Any offer of financial assistance by a foreign national other than close family
- Any request for classified or sensitive unclassified information outside official channels
- Any illegal activity or requests to engage in illegal activity
- Failure of a cleared employee or other trusted individual to report incidents such as those listed above

Information Collection

Consider this scenario. Mark is an analyst for DoD. Lately, he has asked his boss to increase his responsibilities, which in turn would also increase his access. A member of his team thought he saw several classified files in the closet located in Mark's office, though when confronted, Mark denied it. Mark asked yet another coworker to provide a

witness signature for classified files Mark said he destroyed, although the coworker didn't witness the destruction. Should these events be reported?

Before classified or other types of sensitive materials can be passed to a foreign intelligence agency, they must be collected. Information can be stolen, photographed, collected by way of computers or other technology, or obtained through eavesdropping or other surveillance devices. Take a moment to review the incidents listed here that must be reported. Keep in mind this is not a complete list. When in doubt, always err on the side of caution and report the incident.

Report:

- Requests to obtain classified or protected information without authorization
- Requests for witness signatures for destruction of classified information when destruction was not witnessed
- Operating unauthorized cameras, recording devices, computers, or modems in areas where classified data are stored, discussed, or processed
- Presence of any listening or surveillance devices in sensitive or secure areas
- Unauthorized storage of classified material
- Unauthorized access to classified or unclassified automated information systems
- Seeking access to sensitive information inconsistent with duty requirements
- Making statements expressing support of or sympathy for a terrorist group
- Making statements expressing preference for a foreign country over loyalty to the United States
- Expressing radical statements or actions threatening violence against a coworker, supervisor, or others in the workplace

Information Transmittal

Consider this scenario. Saul is a program manager for a U.S. Defense contractor. Saul has taken a lot of vacation lately. When asked about it, he said his father had been sick. However, coworkers later discovered he was traveling to the Middle East. Saul was also seen removing the classified markings from SECRET documents. Should these events be reported?

In the past, the transmittal of classified or sensitive information took the form of stealing documents and physically handing them to the foreign intelligence agent. Spies would photocopy paper materials, take photographs in the workplace, and smuggle materials out in briefcases. While those methods can be and still are used, today there are many more opportunities to transmit information. Technological advances allow the transmittal of large quantities of information without being immediately detected. Personnel must be aware of this problem and, if an illicit transmission is detected, report it immediately.

Take a moment to review the incidents listed here that must be reported. You may encounter signs of information transmittal that are not listed here. When in doubt, always err on the side of caution and report the incident.

Report:

- Unauthorized removal of classified or protected material from the work area
- Use of unclassified computer to transmit classified material
- Improper removal of classification markings from documents
- Discussions involving classified information over a nonsecure telephone
- Concealment of foreign travel

Suspicious Behavior

Consider this scenario. Mary is a DoD employee. Her work schedule has recently changed. While she arrives at her usual time, she doesn't leave until a few hours after her coworkers. Mary also recently traded her economy car for a luxury model. She is also looking for a new home in a prestigious suburb, a significant upgrade from her current small home in a working class neighborhood. Should these events be reported?

There are a number of behaviors that may be connected to CI and security issues. These behaviors require some degree of judgment before reporting. Not everyone fitting this behavior is a spy. There most often are other, plausible alternative explanations for the behavior. It is important that you consider these behaviors while also looking for anomalies. That is, is the behavior a deviation from the person's usual routine or pattern? If you are at all uncertain, it is better to report the behavior than to make no report at all.

Report:

- Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities
- Extensive use of copy or computer equipment to reproduce or transmit classified material that may exceed job requirements
- Repeated or work not required outside of normal duty hours
- Unexplained or undue affluence
- Sudden reversal of financial situation or sudden repayment of large debts
- Attempts to entice personnel into situations that could place them in a compromising position
- Attempts to place personnel under obligation through special treatment, favors, gifts, money, or other means
- Short trips to foreign countries or travel within the United States to cities with foreign diplomatic activities for reasons that appear unusual or inconsistent with a person's interests or financial means
- Indicators of terrorist activity

Reporting Threats

Opening

The events that have occurred at Bob, Sally, James, and John's facilities should all be reported.

Recent events at Bob's facility:

- Unexplained network outages
- Key files missing
- Employees working odd hours
- Unexpected foreign visitors

Recent event at Sally's facility: Unsolicited requests

Recent event at James' facility: Network hacked

Recent event at John's facility: Compromised area

But how do we know *who* to report to and *how* the events should be reported? Let's see.

Who to Report To

When you report threat information, the immediacy of the threat is the first thing you must consider when determining *who* to report to.

All imminent threats—whether DoD facility or personnel or contractor facility—must be reported immediately and directly to the appropriate law enforcement agency, which, in most cases within the United States is the FBI. For cleared defense industry, a copy to DSS is also required. If the threat is not imminent, who you report to depends on your specific location and if you are a military unit or Government contractor.

Specific reporting procedures vary widely across agencies and contractor facilities. Use your agency or facility's reporting procedures to report up your chain of command.

Contractors should submit reports to their DSS Industrial Security Representative (IS Rep) or other cognizant security official.

Contractor reports of espionage, sabotage, terrorism and subversive activity should be sent to the FBI with copies to the IS Rep.

Regardless of the specific procedures you follow, as a best practice, be sure to keep record of the reports you make.

Reports Received by the DSS Counterintelligence (CI) Directorate

The DSS CI Directorate frequently receives threat reports and suspicious contact reports from contractors. When they receive such a report, they will first triage the report to determine its seriousness and priority for action. They will analyze the threat and report to the reporting entity. When warranted, the DSS CI Directorate will release an Intelligence Information Report (IIR) to share the relevant information with the intelligence community and also refer the information to the appropriate authority for investigation as deemed necessary.

For example, national security threats are referred to the FBI. Threats involving possible export violations are referred to U.S. Immigration and Customs Enforcement (ICE). Threats involving items controlled under the International Traffic in Arms (ITAR) are referred to the Department of State. If the contractor is working with the military, the appropriate service investigative agency should be notified.

Information from the suspicious contact reports the DSS CI Directorate receives are is compiled, analyzed, and included in the annual foreign collection trend report.

Other Authorities

Depending on the type of threat and who reports it, military and other agency CI offices may be included in the threat assessment.

Here are some other valuable Federal sources you may wish to consult, though keep in mind that this is not an exhaustive list:

- U.S. Army Intelligence Command (INSCOM)
- U.S. Air Force Office of Special Investigations (OSI)
- Naval Criminal Investigative Service (NCIS)
- Department of Homeland Security (DHS)
- Defense Intelligence Agency (DIA)
- Federal Bureau of Investigation (FBI)
- Department of State Bureau of Diplomatic Security
- The Office of the National Counterintelligence Executive (ONCIX)
- The Interagency OPSEC Support Staff (IOSS)
- U.S. Immigration and Customs Enforcement (ICE)
- U.S. Department of State, Directorate of Defense Trade Controls

Also remember that you will submit your threat reports based on your agency or facility's reporting procedures.

Review Activities

As you know, strange things have been happening at Bob, Sally, James, and John's facilities.

Recent events at Bob's facility:

- Unexplained network outages
- Key files missing
- Employees working odd hours
- Unexpected foreign visitors

Recent event at Sally's facility: Unsolicited requests

Recent event at James' facility: Network hacked

Recent event at John's facility: Compromised area

Since we first met them, additional events have taken place within their facilities.

The following activities will update you with the most recent events. Now that you now know *what* types of behaviors and events must be reported and *how* they should be reported, see if you can determine the best solution for the following situations.

Review Activity 1

Bob has learned more about the recent events at his facility. In view of these new facts, which events should be reported? Select the events that should be reported. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ The employees working odd hours were authorized to do so to complete a deadline that was not widely communicated.
- ☐ The "missing" files were never missing; the employee that reported the incident did not attend a required briefing on the upgrade to a new and authorized file management system.
- ☐ Following an unscheduled visit by personnel not well known to the facility, personnel at Bob's facility discovered papers outlining bomb-making instructions and dates and locations where the devices would be placed.
- ☐ The recent network outages were traced back to the addition of new, authorized hardware. The system has since been upgraded and the issue is resolved.

Review Activity 2

Bomb-making instructions were found at Bob's facility. Things are also happening at Sally, James, and John's facilities. Which events should be reported? Select the events that should be reported. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Personnel at Sally's facility have unknowingly shared a crucial technical component of missile technology.
- ☐ Network administrators at James's facility discover that detailed diagrams of U.S. military bases have been compromised.
- ☐ Export-restricted material is missing from a restricted area in John's facility.

Review Activity 3

Bob, Sally, James, and John know they must report these events. To whom should they report? Write in FBI or Agency/Facility Chain of Command for each statement. Then check your answers in the Answer Key at the end of this Student Guide.

_____	Personnel at Bob's facility discovered papers outlining bomb-making instructions and dates and locations where the devices would be placed.
_____	Personnel at Sally's facility have unknowingly shared a crucial technical component of missile technology
_____	Network administrators at James's facility discover that detailed diagrams of U.S. military bases have been compromised.
_____	Export-restricted material is missing from a restricted area in John's facility.

Lesson Conclusion

Summary

In this lesson, you have learned that reporting threat information is essential. You have learned that lesser threats at your facility may be a small piece of a larger picture. You should now know which types of events and behaviors are reportable, and to whom you should report.

Answer Key

Review Activity 1

- ☐ The employees working odd hours were authorized to do so to complete a deadline that was not widely communicated.
- ☐ The "missing" files were never missing; the employee that reported the incident did not attend a required briefing on the upgrade to a new and authorized file management system.
- ☑ Following an unscheduled visit by personnel not well known to the facility, personnel at Bob's facility discovered papers outlining bomb-making instructions and dates and locations where the devices would be placed. (correct answer)
- ☐ The recent network outages were traced back to the addition of new, authorized hardware. The system has since been upgraded and the issue is resolved.

Review Activity 2

- ☑ Personnel at Sally's facility have unknowingly shared a crucial technical component of missile technology. (correct answer)
- ☑ Network administrators at James's facility discover that detailed diagrams of U.S. military bases have been compromised. (correct answer)
- ☑ Export-restricted material is missing from a restricted area in John's facility. (correct answer)

Review Activity 3

The immediacy of a threat is subjective. If there is ever any doubt about a threat's immediacy, report directly to the FBI.

FBI	Personnel at Bob's facility discovered papers outlining bomb-making instructions and dates and locations where the devices would be placed.
Chain of Command	Personnel at Sally's facility have unknowingly shared a crucial technical component of missile technology
Chain of Command	Network administrators at James's facility discover that detailed diagrams of U.S. military bases have been compromised.
Chain of Command	Export-restricted material is missing from a restricted area in John's facility.

Job Aid: Examples of Reportable Events or Behaviors

The following is not intended to be an exhaustive list. When in doubt, report an event or behavior.

Recruitment

Report suspicious events or behaviors including, but not limited to:

- Contact with an individual associated with a foreign intelligence, security, or terrorist organization
- Failure to report an offer of financial assistance by a foreign national other than close family
- Failure to report a request for classified or unclassified information outside official channels
- Engaging in illegal activity or a request to do so

Information Collection

Report events or behaviors including, but not limited to:

- Requests to obtain classified or protected information without authorization
- Requests for witness signatures for destruction of classified information when destruction was not witnessed
- Operating unauthorized cameras, recording devices, computers, or modems in areas where classified data are stored, discussed, or processed
- Presence of any listening or surveillance devices in sensitive or secure areas
- Unauthorized storage of classified material
- Unauthorized access to classified or unclassified automated information systems
- Seeking access to sensitive information inconsistent with duty requirements

Information Transmittal

Report suspicious events or behaviors including, but not limited to:

- Unauthorized removal of classified or protected material from the work area without appropriate authorization
- Use of unclassified computer to transmit classified material
- Improper removal of classification markings from documents
- Discussions involving classified information over a nonsecure telephone
- Concealment of foreign travel

Suspicious Behavior

Report behavior including, but not limited to:

- Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities
- Extensive use of copy or computer equipment to reproduce or transmit classified material that may exceed job requirements
- Repeated or unrequired work outside of normal duty hours
- Unexplained or undue affluence
- Sudden reversal of financial situation or sudden repayment of large debts

- Attempts to entice DoD personnel into situations that could place them in a compromising position
- Attempts to place DoD personnel under obligation through special treatment, favors, gifts, money, or other means
- Short trips to foreign countries or travel within the United States to cities with foreign diplomatic activities for reasons that appear unusual or inconsistent with a person's interests or financial means

Derived from NISPOM Section 1-301 and 1-302 a and b, and DoDD 5240.06 Enclosure 4

Student Guide

Course: Integrating Counterintelligence (CI) and Threat Awareness into Your Security Program, v2

Lesson: Course Conclusion

Contents

Course Summary

Incorporating counterintelligence (CI) and threat awareness into your security program makes your program stronger and more successful. Working with credible, current threat information is needed to meet security requirements and to engage the risk management process.

You should now know that to protect your facility and its information and personnel, you must be aware of the types of threats that exist and how your adversaries operate. You must seek out and obtain threat information from a variety of sources and it is essential that you report threats that you encounter.

Lesson Review

Here is a list of the lessons in the course:

- Introduction to Counterintelligence (CI) and Threat Awareness
- Identifying Threats
- Obtaining Counterintelligence (CI) and Threat Information
- Reporting Counterintelligence (CI) and Threat Information

Course Objectives

You should now be able to:

- ✓ Identify the purpose of incorporating CI and threat awareness information into a security program
- ✓ Identify CI and threat awareness policy requirements for Industry and DoD personnel
- ✓ Identify the role of the DSS CI Directorate
- ✓ Identify the role of threat identification in the analytical risk management process
- ✓ Identify key types of threats and common methods of operation
- ✓ Identify information most likely to be targeted by espionage
- ✓ Identify key sources of threat information
- ✓ Identify the types of CI and threat awareness information that should be reported
- ✓ Identify CI and threat information reporting requirements and procedures

Conclusion

Congratulations. You have completed the Integrating CI and Threat Awareness into Your Security Program course.

To receive course credit, you must take the Integrating CI and Threat Awareness examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.