Protecting Assets in the NISP

Table of Contents

Course Introduction

Security Breach

Today DoD officials reported that design and capability details of the new explosives detection and disarmament robot known as ODAD were obtained by foreign operatives. The security breach was traced to Automated Explosives Detection Technologies, commonly referred to as AEDT, a locally based government contractor. The ODAD contract has reportedly been cancelled due to this compromise. Last year AEDT was awarded the five-year contract to provide parts and services supporting the development of the robot.

Initial reports indicate the breach of security occurred at AEDT when known foreign intelligence entities targeted the company by following the company at trade shows, attending the company's presentations at academic functions, and through requests for information from the company.

Foreign operatives collected unclassified information from the company over time and pieced this information together to discover classified details of the new robot. AEDT will reportedly lose up to 10 million dollars from the loss of this government contract and may find it difficult to compete for other government contracts in the near future.

The damage from this security breach will affect over 60 AEDT employees here in the local area.

Your company CEO, Doug Freeman, has stopped by your office.

Did you see that news clip? That company's technology is not that different from ours! As my Facility Security Officer, I'm expecting you to prevent a similar situation at our facility. I expect to see a comprehensive plan to integrate counterintelligence awareness into our security program by the end of the week.

Course Structure and Learning Objectives

Welcome to the Protecting Assets in the NISP Course. What you've just seen is an extreme example of what can happen when a company does not have an effective security program that incorporates counterintelligence awareness. Industry partners must understand that the assets they're protecting identify threats from foreign intelligence entities, recognize their vulnerabilities, and deploy countermeasures to mitigate risk to their organization and to national security. This training is delivered as a scenario in which you are the Facility Security Officer, also known as an FSO, for a company within the National Industrial Security Program, or NISP for short. The course consists of three lessons and should take approximately one hour to complete. Here are the course learning objectives.

Course Structure and Objectives

Lesson: Introduction to Counterintelligence (CI) and Threat Awareness

- Identify the purpose of CI and threat awareness in a security program, Department of Defense (DoD) policy requirements for industry, and the role of analytical risk management in risk mitigation.

Lesson: Identifying Threats

- Identify sources of threat information, recognize types of threats, common methods used to collect information, and identify the role of the Defense Counterintelligence and Security Agency (DCSA) directorate in CI awareness.

Lesson: Countermeasures and Reporting

- Define countermeasures, identify the purpose of foreign travel and foreign visit programs, describe CI training requirements for industry, and explain reporting requirements.

Introduction to CI and Threat Awareness

Lesson Introduction

Your CEO has asked you to create a Counterintelligence Integration Plan for your company.

You decide to begin by researching the purpose of counterintelligence and threat awareness, why they are important to your security program, how the Defense Counterintelligence and Security Agency, or DCSA, can assist companies like yours, the policies, and requirements that you must satisfy, and how the analytical risk management process can be used to mitigate risk in your facility.

You have several resources from which you can gather information to create your plan for integrating counterintelligence into the security program. These resources include the DCSA Industrial Security Representative, or IS Rep, the NISP Operating Manual, or NISPOM, and risk management procedures.

Counterintelligence Integration Plan
Today's objectives

- Identify the purpose of incorporating CI and threat information into a security program.
- Identify CI and threat awareness policy requirements for industry.
- Identify the role of analytical risk management in risk mitigation.

Meeting the IS Rep

Hello! This is Ryan. I'm so glad you reached out to me.

DCSA oversees the protection of U.S. and foreign classified information and technologies in the hands of cleared industry under the National Industrial Security Program by providing professional risk management services.

An effective security program is key to the company's ability to retain its clearance, to get and maintain government contracts, and to remain competitive in the marketplace. Having a Counterintelligence or CI program in place is fundamental to the success of your security program. Since you are close by, let's get together and talk about how you can integrate CI and threat awareness into your security program.

What is Counterintelligence?

Hi there! Thanks for coming over. As I started to tell you on the phone, in order to integrate CI and threat awareness information into a security program, you need a strong understanding of what counterintelligence is and what it should achieve. So, what is CI? Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements hereof, foreign organizations or persons, or international terrorist activities.

In your role as a security professional, you support counterintelligence by implementing security countermeasures to defeat foreign collection activity and by reporting suspicious contacts to the appropriate counterintelligence support team.

Working together, security and CI support national security and protect valuable company assets from theft and compromise.

How does CI Complement Security?

How do CI and security relate to each other? CI and security are mutually supportive with shared goals and responsibilities associated with protecting critical resources and sensitive information.

	Security	CI
Focus	Establishing standards Fixing weaknesses	Identifying, understanding, and countering collection efforts
Objective	Reduce vulnerability	Prevent, detect, and respond to threats
Perspective	Examines the company's activities and assets from the company's leadership perspective	Examines the company from the adversary's perspective

Security focuses on establishing standards, adhering to those standards, and fixing weaknesses. CI focuses on identifying, understanding, and countering adversary collection efforts.

The objective of security is to protect assets and reduce vulnerability. The objective of CI is to prevent, detect, respond to and sometimes exploit foreign intelligence entity threats.

Security looks at the company from the inside-out - examining the company's activities and assets. CI takes an outside-in perspective – examining the company from the adversary's perspective. Together, security and CI provide greater protection for your company's operations and assets. Therefore, your goal is to help your company develop strong practices in both security and CI.

Security and CI Activities

Examples of incorporating CI into the security program include identifying and prioritizing assets that need protection; assessing risk, threat and vulnerability; sharing threat information; and deploying appropriate security countermeasures; identifying suspicious contacts and filing Suspicious Contact Reports, or SCRs, with DCSA and/or FBI as warranted; responding to cyber notifications and maintaining strong cybersecurity practices; conducting foreign travel briefings and debriefings for employees who travel; implementing a foreign visit program; establishing an insider threat program; and providing CI and insider threat awareness and security briefings in accordance with the NISPOM.

The Facility Security Officer and Counterintelligence

FSOs are responsible for protecting sensitive and classified information and technology within their companies. But, what does that really mean?

While strong physical security is important, not all losses, thefts, and compromises of sensitive and classified information and technology involve obvious breaches of physical security.

Foreign intelligence entities and commercial adversaries have devised methods to steal technology that is protected by robust physical security measures. It is essential that you recognize how modern adversaries operate – and learn appropriate responses to counter their efforts.

Integrating CI and threat awareness into your security program allows you to gain a better understanding of the threats facing your company and develop the best measures to protect your company's valuable assets.

Elements of a Successful CI Program

There are several elements that we must consider and include in your CI program. I see that you have your FSO Handbook. Good thinking.

Let's talk about some of the elements that contribute to a successful CI program and you can add that information to your FSO Handbook to help build the CI Program and awareness at your facility.

The foundation of your CI program relies on a risk-based approach and working with DCSA to ensure that it is aware of and can help you when issues arise. Senior leadership support and employee awareness are at the center of a successful CI program.

Your company must have a strong cybersecurity program to protect your information systems. You must also be vigilant and have programs in place to address both foreign travel and foreign visitors.

The CI program must take into account any special programs requiring protection, for example, Special Access Programs or Critical Program Information.

A strong and continuously integrated insider threat program is essential because your company can be most vulnerable from those with authorized access.

The most critical element is reporting. You must not only learn to recognize suspicious activity but to report it in a timely manner to your DCSA CI Special Agent and/or the FBI as required. This reporting allows these elements to conduct counterintelligence actions in defense of your company and national security.

Senior Leadership Support
Senior leadership includes, but is not limited to, the following positions:

- Chief Executive Officer
- Chief Financial Officer
- Chief Information Officer
- Office of General Counsel
- Office of Information Assurance
- Office of Human Resources, and/or
- Office of Security
- Other Key Management Personnel

Strong Cybersecurity Program

- Establish a resilient cyber defense posture
- Enhance cyber situational awareness
- Assure survivability against complex cyber attacks

SAP/Critical Program Information Protection
Elements of effective Special Access Program/Critical Program Information Protection:

- Program Protection Plan
- Technology Control Plan (TCP)
- Classification Guide
- Current threat assessments
- Additional guidance on DD Form 254, DoD Contract Security Classification Specification
- Protect Critical Program Information (CPI) as required in contracts, DoDI 5200.39, and DoDI 5240.19.

Insider Threat Program

An effective CI program should integrate CI into a company-wide insider threat program that includes company leadership, information technology, security, legal, human resources, and ethics personnel.

Elements of an Insider Threat Program:

- Identification of Insider Threat Program Senior Official
- Training for Program Manager and Insider Threat Team members
- Initial and annual insider threat awareness training for cleared employees
- Information technology (IT) system monitoring and auditing program

- Records maintenance
- Existence of and adherence to insider threat reporting procedures
- Existence of an Insider Threat Policy
- Leadership support
- Self-Assessments of the Insider Threat Program

Parting thoughts from the IS Rep

DCSA oversees the protection of U.S. and foreign classified information and technologies in the hands of cleared industry under the National Industrial Security Program, or NISP, by providing professional risk management services. The NISPOM, outlines the measures you are required to take to protect national assets in your facility.

However, NISPOM compliance is just a start.

A truly effective security program will take into consideration the principles of risk management. These efforts identify your critical assets, determine the threats against them, identify vulnerabilities at your facility that an adversary is likely to exploit, and help you find effective countermeasures. If you haven't already, review the risk management information. You know, threats from foreign intelligence entities, insiders, and others are very real and affect companies like yours every day. I recommend you review the elements of the NISPOM that outline your requirements in these areas.

NISPOM - Special Requirements for Contractors

Now that we know why we should incorporate CI and threat awareness into your security program, let's look at the policies related to CI that industry must understand and follow.

These requirements are covered in DoD 5220.22-M, National Industrial Security Program, or NISPOM.

The NISPOM controls disclosure of classified information by the Federal Government and DoD agencies to their contractors and establishes safeguards for special classes of information.

Let's go back to your handbook and look at more information on the NISPOM.

The NISPOM requires that adverse information concerning cleared employees and any suspicious contacts be submitted to the DCSA. In addition, actual, probable, or possible espionage, sabotage, terrorism, or subversive activities must be reported to both the DCSA and the FBI. You must also provide annual and refresher Insider Threat and security training and make available reports associated with training completions.

DCSA issues Industrial Security Letters, or ISLs, to keep cleared contractors, government contracting activities, and DoD activities aware of developments relating to industrial security. These letters provide information and clarification of existing policies and requirements. ISLs have been issued for reportable events.

ISL 2019-01 implements Security Executive Agent Directive 4 or SEAD 4, National Security Adjudicative Guidelines, and additional reporting requirements for foreign travel.

ISL 2016-02 provides clarification and guidance to assist contractors as they establish and tailor an insider threat program to meet NISPOM 1-202 requirements.

ISL 2013-05 requires contractors to report activities that meet the threshold for reporting, including activities that may have occurred on its unclassified information systems.

ISLs 2006-01 and 2006-02 explain the major changes implemented with the 2006 NISPOM revision.

All of these ISLs can be found in the NISP Library but they are also available in your handbook for review.

Finally, you should collaborate with your leadership to establish standard operating procedures to specify how employees will accomplish specific requirements from the NISPOM.

The Role of Analytical Risk Management in Identifying Threats

Your ability to protect your company's information, technology, and personnel depends on your ability to understand and identify threats. When you weave CI into your security program, you are improving your facility's ability to manage risk.

A successful CI program adopts a risk-based approach to enhanced CI awareness for information, programs, and personnel most likely to be targeted or vulnerable to foreign/competitor collection efforts. Let's briefly look at the analytical risk management process and the goal of each step.

The risk management steps are:

- Identify assets and determine the impact of loss or compromise
- Identify threats
- Identify vulnerabilities
- Assess risk, and
- Develop and apply countermeasures

Identify Assets and Impact of Loss

To protect against threats, you must consider all sensitive assets – both classified and unclassified. Assets include people, information, equipment, facilities, activities and operations, and suppliers, or PIEFAOS.

You must protect any asset, that if compromised would significantly damage national security, alter program direction, compromise the program or system capabilities, shorten the expected life of the system, or require research, development, testing, and evaluation to counter the impact of loss.

Identifying Threats

Identify the threats to your company. This means attempting to determine who the adversaries of your company and the Government programs you support are, determining who wants to gain

unauthorized access to information that you protect, and determining the capabilities and intentions of these adversaries.

Identify Vulnerabilities

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.

Risk Assessment Checklist

- Cybersecurity
- People
- Technology
- Contractual
- Supply chain
- Operations
- Environmental
- Product liability

Assess Risk

Now think about the impact of your assets being compromised. What is the worst that could happen? Loss of economic market? Loss of strategic and military advantage? Loss of jobs? Or loss of life? This impact, coupled with the probability that an adversary has both the intent and capability to exploit the particular vulnerability, determines risk.

Develop and Apply Countermeasures

Finally, you must think about actions or countermeasures that you can develop and apply to mitigate risk. Countermeasures may be specific to the threats and vulnerabilities identified.

Here are a couple of examples. When high-risk and targeted personnel or programs are identified, you can administer additional security and CI awareness training that is specific to these individuals or programs. Or if your risk is increased because of participation in a conference, trade show, or seminar, you can implement counterintelligence threat awareness briefings and debriefings for attendees. The success of your security program depends on your ability to develop and apply such countermeasures.

Knowledge Check Activity

Question 1 of 5
CI is the information gathered and activities conducted to protect against what?
Select all that apply.

- □ Espionage, sabotage, terrorism
- □ Assassinations conducted for or on behalf of foreign governments, organizations, or persons
- □ Activities by large companies to obtain operating capital within a foreign country
- □ International terrorist activities

Answer: CI is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements hereof, foreign organizations or persons, or international terrorist activities.

Question 2 of 5
Integrating CI and threat awareness into a security program helps to accomplish which of the following?
Select all that apply.

- □ Assist DoD in maintaining a tactical advantage over foreign intelligence operatives
- □ Protect valuable company assets from loss and compromise
- □ Identify which assets need protecting
- □ Establish countermeasures

Answer: The goals of including CI in a security program are to protect sensitive company assets from loss and compromise, identify which assets need protecting, and to establish countermeasures.

Question 3 of 5
DoD 5220.22-M NISPOM does which of the following for industry?
Select all that apply.

- □ Controls the disclosure of classified information to contractors
- □ Identifies the cost associated with particular contracts
- □ Protects special classes of classified information
- □ Requires contractors to hire counterintelligence special agents

Answer: Controls the disclosure of classified information to contractors; Protects special classes of classified information

Question 4 of 5
The NISPOM requires that adverse information concerning cleared employees and any suspicious contacts be reported to DCSA.
Select the best answer.

- o True
- o False

Answer: That statement is true. The NISPOM requires that adverse information concerning cleared employees and any suspicious contacts be reported to DCSA.

Question 5 of 5
CI helps security officials to manage risk in which of the following ways? Select all that apply.

- □ Focus on assets and identify the threats to them
- □ Identify vulnerabilities
- □ Develop and apply countermeasures
- □ Develop investigation procedures
- □ Develop security classification guides

Answer: CI helps security officials to manage risk by focusing on assets and identify the threats to them, identifying vulnerabilities, and developing and applying countermeasures.

Lesson Summary

Well, that wraps up your familiarization with CI and threat awareness. You used available resources to learn the purpose of CI and threat awareness in your security program, the policies and requirements that you must follow, and how analytical risk management can be used in CI awareness.

You have learned quite a bit from your research today. Let's have a look at what information you have collected for our CI Integration Plan. You can update this information in your FSO Handbook as you continue your familiarization with CI and threat awareness.

Components to include in the CI integration plan

- Implement NISPOM policy
- Obtain Senior Leadership Support
- Establish a Risk-Based Approach to CI
- Provide Employee Awareness
- Create a Strong Cybersecurity Program
- Establish SAP/Critical Program Information Protections
- Integrate the Insider Threat Program
- Establish reporting guidelines according to the NISPOM

Identifying Threats

Introduction to Identifying Threats

According to your calendar, you have set aside time to continue gathering information for your CI Integration Plan.

Today you will research types of threats, which employees are most vulnerable to targeting by foreign intelligence entities, common methods used to collect information and technology, and key sources available for us to gather threat information.

You have already identified resources for your research.

When you complete your research, you should be able to update your CI Integration Plan.

Sources of Threat Information: Government

Information about potential threats is all around us. It's up to us to seek it out and learn from it. Threat summaries and intelligence reports can provide an overall picture of the threat, though it's important to place this information into context for your specific facility.

Government Contracting Activity

For government contractors, the Government Contracting Activity, or GCA, is a good source for obtaining threat information. Individuals within the GCA such as the Contracting Officer's Representative, or COTR; the Security Officer; or the appropriate Military Department or DCSA CI Special Agent may be able to provide us with contract-specific threat information and threat assessments that identifies what your facility has or does that makes it a target.

DCSA CI Directorate

Recall that the DCSA CI Directorate publishes an annual trend report that summarizes the threat reports received from cleared contractor facilities and provides information that shows trends related to what is targeted and the methods used.

You must familiarize yourselves 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? Classified editions of these reports, which contain more detailed information, are available from the DCSA CI Directorate to security professionals with appropriate clearance and need-to-know.

Federal Bureau of Investigation (FBI)

The Federal Bureau of Investigation, or FBI, has primary responsibility for counterintelligence investigations within the United States.

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.

You can use the FBI resources that provide threat information related to espionage, counterintelligence, counterterrorism, economic espionage, cyber and physical infrastructure protection, and all national security issues.

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. Keep in mind that this is not an exhaustive list. You must seek out information from whatever sources are appropriate based on your facility's capabilities and the threats it may face.

Other Federal, State, and Local Agencies

- Department of Homeland Security (DHS)
- Defense Intelligence Agency (DIA)
- Department of State Bureau of Diplomatic Security
- National Counterintelligence and Security Center (NCSC)
- The Interagency OPSEC Support Staff
- State and local law enforcement agencies

The Role of DCSA Counterintelligence Directorate in CI and Threat Awareness

The DCSA Counterintelligence Directorate provides CI functional services to cleared industry and is a key resource for your company. The DCSA CI Directorate provides early detection and referral of potential espionage, technology transfer, trade secret theft, and other matters to applicable intelligence, counterintelligence, and/or law enforcement entities. These entities may also assist industry in the recognition and reporting of collection attempts by foreign intelligence entities or FIEs. The DCSA CI Directorate also publishes threat information annually and makes it available to industry, and advises and assists industry partners in the development and implementation of countermeasures.

DCSA Resources Available to the FSO

Having a CI strategy requires you to understand the sensitive and classified information, technology, and systems that need to be protected within your facility, and the sources and nature of threats to your facility.

DCSA has several resources available that outline threats to cleared industry. The main one is an annual publication, Targeting U.S. Technologies. This report consolidates and presents the threat information DCSA learned over the past year, organized in various ways—to include by region, by methods of operation, and by technology. Remember to update these resources in your handbook.

Each facility also has an assigned DCSA CI Special Agent. Your CISA can provide specific, even classified information, about threats to your facility.

Finally, you can always reach out to your facility's Industrial Security Representative, or IS Rep, for assistance. IS Reps provide oversight and assistance to cleared contractor facilities in ensuring the protection of national security information.

DCSA's ability to provide accurate threat information depends on the information that industry reports about the suspicious contacts and activities that your facility and personnel experience.

Sources of Threat Information: Open Sources

While obtaining threat information from Government sources is preferred, there are open sources of threat information. Open sources of threat information include commercial sources such as news media, the internet, and publications from other companies and foreign governments. You should seek out threat information from whatever sources that best suit your organization's needs.

Work with your IS Rep and CISA to identify sources that are appropriate for your organization. If you choose to use open sources, always check the validity of the information with your IS Rep, the FBI, or other government agency.

What are Types of Threats Facing Industry?

Threats to your facility are diverse, dynamic, and complex.

These threats may arise from people that have legitimate access to your company.

This includes company employees, consultants, subcontractors, and custodial personnel.

Some threats may come from your daily business associations. These types of threats may be business competitors, criminal activities disguised as authentic business activities, or insider threats. Other threats originate in foreign countries and can include government, quasi-governmental activities, companies, and individuals.

Insider Threat

Insider threat is the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information. Source: DoD 5220.22-M, NISPOM

An effective CI program should integrate CI into a company-wide insider threat program that includes company leadership, information technology, security, legal, human resources, and ethics personnel.

Business Competitors

A business competitor is a company in the same industry or a similar industry which offers a similar product or service

Companies with whom you compete for business may use questionable or illegal means to get the upper hand in business. Competitors' tactics may involve targeting your assets in the same manner as an FIE.

Criminal Activities

Criminal activities are persons or groups attempting to exploit lapses in physical security to obtain protected information or products with no pretense of legitimate acquisition

FIEs and terrorists may affiliate themselves with others involved in criminal activity to make contacts and obtain information or technology.

Threats from FIEs

Threats from FIEs
FIE can include:

- State sponsored foreign intelligence activities or other government organizations
- Foreign commercial organizations
- Quasi-governmental organizations such as universities and research centers, or individuals

FIE can include any foreign organization, person, or group that conducts intelligence activities to acquire information, influence the company's activities, or disrupt the company's mission or goals.

Terrorist Organizations

A terrorist group is a group that threatens the security, infrastructure, or citizens of a nation or community by planning and carrying out acts of terror

Terrorist organizations may seek to disrupt the economy, degrade national security, or cause fear within the general population.

Targeted Technology and Information

Now that you understand who may target you, let's discuss what the FIEs are after. Technology, information, and employees may all be targets.

Recall that DCSA provides an annual report with threat information. That report also identifies the most highly targeted assets. According to the current DCSA trend analysis, in recent years, the most targeted technologies are command, control, communication, and computers, also known as C4, aeronautic systems, electronics, optics, radars, armaments, marine systems, software, and materials. As you can see, both classified and unclassified technologies are targeted.

Remember, most programs are targeted at one time or another. It's critical to understand that your technology may not be targeted as frequently, but that even one loss can have a negative impact on national security and your bottom line.

You can review the Industrial Base Technology List to learn the systems, equipment, and materials found in each category.

Areas Targeting U.S. Technologies

Trend analysis of recent reporting to DCSA reflects a continued rise in reported suspicious contact attempts to obtain sensitive or classified information and technology from industry. Based on reporting to DCSA, all geographic regions are known to target U.S. Defense technology.

East Asia and the Pacific entities have remained the most significant collectors of sensitive or classified U.S. technology and information. Europe and Eurasia also represent a significant threat. Entities from the Near East are also active collectors of sensitive or unclassified technology and information.

While you see fewer reports from the Western Hemisphere and Africa, threat actors are still present in this region. As you can see, foreign collectors from all nations target both classified and sensitive U.S. technology and information. It's important to recognize suspicious behaviors and activities that may represent collection attempts regardless of the source. So, let's talk about the methods of contact and methods of operation that might be used in concert as collection methods to illicitly acquire information and how you might recognize collection activities.

Methods of Contact and Methods of Operation

A collection method is at the intersection of a method of contact and method of operation. DCSA CI has identified 12 methods of contact and 13 methods of operation employed by our foreign adversaries to achieve a collection or intelligence objective.

A method of contact is the approach used to connect the foreign actor to the targeted individual, information, network, or technology in order for the foreign actor to execute the method of operation.

A method of operation is a distinct pattern or method of procedure thought to be characteristic of or habitually followed by an individual or organization involved in criminal or intelligence activity.

There is more information on the methods of contact and methods of operation in the course resource page.

Foreign Collection Methods

To manage risk associated with targeting of your facility and its assets, you must be knowledgeable of collection methods based off of methods of contact and methods of operation used to collect information, indicators that attempts are being made to collect information, and potential countermeasures.

According to DCSA analysis, the most common foreign collection methods used in over 80% of targeting cases are requests for information; academic solicitation; suspicious network activity;

targeting at conferences, conventions, and trade shows; seeking employment; foreign visits; and elicitation and recruitment.

The nature and extent of industry reported suspicious contacts suggest a concerted effort to exploit cleared contractors for economic and military advantage. These contacts range from outright attempts to steal technology to seemingly innocuous business ventures. Targeting indicators are signs that an individual or group may be involved in the illegal collection of information on behalf of an FIE. As part of your overall risk management strategy, you will implement countermeasures to mitigate the risk associated with foreign collection methods. Countermeasures are the employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities.

Please note that this is not an exhaustive list of collection methods and does not cover every method of contact or method of operation. These reflect the most common methods our adversaries employ. More information on our adversaries' techniques can be found in the resource pages, on CDSE.edu, or by contacting your local CISA.

Let's look at each of the collection methods, their indicators, and potential countermeasures.

Foreign Collection Methods: Requests for Information

Requests for information is an attempt to collect protected information by directly or indirectly asking, requesting, or eliciting the protected information.

Requests for Information: Techniques

Requests for information are normally unsolicited and often originate from unknown sources like foreign companies, individuals, or foreign government officials or quasi- government organizations.

Requests for Information: Methods of Operation

The most common methods of operation used in requests for information are RFI/Solicitation, Exploitation of Experts, Exploitation of Supply Chain, and the Exploitation of Business Activities.

Requests for Information: Methods of Contact

The most common methods of contact are Email; Social or Professional Networking; and Conferences, Conventions and Tradeshows.

Requests for Information: Targets

These requests often target business developers, sales, marketing, subject matter experts or SMEs, and Information Technology or IT, personnel.

Requests for Information: Indicators

Requests for information are often submitted by email and may ask for technical information or technology capabilities.

Requests might come from a foreign address, the requestor may provide identification as a student or consultant, claim employment with a foreign government, or claim that work is being performed on behalf of a foreign government or program.

Other requests might ask for or about technology related to a defense program or say that it's ok for you to share the information with them. FIEs are continuously changing their methods of operation. This list only identifies those methods that have most often been observed and reported.

More Examples:

- 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
- Advises the recipient to disregard the request if it causes a security problem, or the request is for information the recipient cannot provide due to security classification, export controls, etc.
- Advises the recipient not to worry about security concerns
- Assures the recipient that export licenses are not required or not a problem
- Fails to identify the end user

Requests for Information: Countermeasures

We should view direct but unsolicited requests as suspicious - especially if they are delivered through the internet. We must release information only to people or groups for which you can verify their identity, address, and authorization to access the information requested.

Finally, if you cannot verify the request or if the request is suspicious, do not respond to the request in any way and immediately report the incident to the FSO or other security personnel.

Foreign Collection Methods: Academic Solicitation

Academic solicitation is an effective way of collecting information because of the collaborative nature of the academic community. FIEs attempt to collaborate with U.S. research institutions under the guise of legitimate research. This method offers FIEs access to developing technologies and cutting-edge research that not only may satisfy their immediate technological requirements but may provide them better educated scientists and researchers for their indigenous technology development.

Academic Solicitation: Techniques

Academic solicitation uses students, professors, scientists, or researchers as collectors improperly attempting to obtain sensitive or classified information.

Academic Solicitation Techniques

- Foreign Universities or Academic Centers
- Individuals overseas or placed in the U.S.
- Quasi-governmental Organizations, such as research centers and institutes

Academic Solicitation: Methods of Operation

The most common methods of operation used in Academic Solicitation are the Exploitation of Experts and Resume Submissions.

Academic Solicitation: Methods of Contact

The most common methods of contact are Email; Social or Professional Networking; and Conferences, Conventions and Tradeshows.

Academic Solicitation: Targets

This method targets universities, Government, private research facilities, cleared facilities, admissions departments, SMEs, professors, and faculty members.

Academic Solicitation: Indicators

Collection for this method often involves applications for admission to advanced science, technology, engineering, and math degree programs associated with cleared facilities, requests for review of academic papers, or requests for study or consult.

More Examples include:

- Foreign students accepted to a U.S. university or at postgraduate research programs are recruited for their collection efforts.
- U.S. researchers receive requests to provide dual-use components under the guise of academic research.
- U.S. researchers receive unsolicited emails from peers in their academic field soliciting assistance on fundamental and developing research.
- U.S. professors or researchers are invited to attend or submit a paper for an international conference.
- Overqualified candidates seeking to work in cleared laboratories as interns.
- Candidates seeking to work in cleared laboratories whose work is incompatible with the requesting individual’s field of research.
- Subject matter experts (SMEs) receive requests to review research papers in hopes the SME will correct any mistakes.

Academic Solicitation: Countermeasures

As with requests for information, you should view academic solicitations received via the internet with suspicion. Respond only to people whose identity and address can be verified. Ensure that all responses include only information authorized for release.

Foreign Collection Methods: Suspicious Network Activities

Suspicious network activity is the fastest growing collection method for foreign entities seeking to gain information about U.S. interests.

Suspicious Network Activities: Techniques

FIEs may introduce corrupted or falsified data, malware, malicious code, or viruses into information systems. FIEs may also directly hack a system, elicit information from chat rooms, or email solicitations, also known as phishing.

Suspicious Network Activities: Methods of Operation

The most common method of operation used in Suspicious Network Activity is the Exploitation of Cyber Operations.

Suspicious Network Activities: Methods of Contact

The most common methods of contact are Phishing Operations and Cyber Operations.

Suspicious Network Activities: Targets

An FIE may target anyone or any system at any facility and may employ multiple techniques within a given target.

Suspicious Network Activities: Indicators

Major indicators of attempted collection include unauthorized attempts to access a system, receiving emails from foreign addresses, unauthorized or unplanned hardware or software modifications, unauthorized data storage or transmission, unauthorized system access to or disclosure of information, and any acts that interrupt or result in a denial of service.

Suspicious Network Activities: Countermeasures

Guarding against this type of collection attempt requires aggressive and continuous countermeasures. You should develop and implement a Technology Control Plan, or TCP. You must conduct audits at least weekly and optimally, daily instead of relying on firewalls for protection against all attacks. You must always report intrusion attempts, avoid responding to or clicking on links from unknown sources, and disconnect computer systems temporarily if there is a severe attack.

Foreign Collection Methods: Targeting at Conferences, Conventions, and Trade Shows

This method of collection links the targeted programs and technologies with the knowledgeable personnel. Your personnel can be targeted at any conference, convention, or trade show – foreign or domestic.

Targeting at Conferences, Conventions, and Trade Shows: Techniques

Technical experts may be contacted to share their expertise or asked to share restricted, proprietary, or classified information.

Targeting at Conferences, Conventions, and Trade Shows: Methods of Operation

The most common method of operation used at conferences, conventions, and tradeshows are the Exploitation of Business Activities, RFI/Solicitation, the Exploitation of Experts, and the Attempted Acquisition of Technology.

Targeting at Conferences, Conventions, and Trade Shows: Methods of Contact

The most common methods of contact are Conferences, Convention, and Tradeshow solicitations and Personal Contact.

Targeting at Conferences, Conventions, and Trade Shows: Targets

Experts may receive all-expense-paid invitations to lecture or requests for briefing materials many months in advance of scheduled presentations.

Indicators Prior to event include:

- Personnel receive an all-expenses-paid invitation to lecture in a foreign country
- Requests for a presentation summary or brief 6 – 12 months prior to the lecture date
- Host unsuccessfully attempted to visit facilities in the past
- Travel to event may pose targeting opportunities

Targeting at Conferences, Conventions, and Trade Shows: Indicators During an Event

During events, there may be excessive or suspicious photography or filming of technology and products, or casual conversation after the event suggesting future contacts or relationships.

More Examples include:

- Telephone monitoring and hotel room intrusions
- Conversations involving classified, sensitive, or export-controlled technologies
- Foreign attendees' business cards do not match stated affiliations
- Attendees wear false name tags
- Individuals returning to same booth multiple times
- Detailed and probing questions about specific technology

Targeting at Conferences, Conventions, and Trade Shows: Countermeasures

FSOs can provide employees with detailed travel briefings concerning the threat, precautions to take, and how to react to elicitation before the employees travel and debrief them upon their return. At the company level, you can plan what, when, where, and with whom you are sharing information. We can even take mock-ups to these events instead of the actual equipment.

More Examples include:

- Request a threat assessment from the program office
- Report intrusion attempts
- Restrict information provided to only what is necessary for travel and hotel accommodations
- Carefully consider whether equipment or software can be adequately protected
- Debrief attendees after the event to identify potential suspicious activity

Foreign Collection Methods: Foreign Visits

Foreign visits can result in the loss of technology or information or lay the ground work for targeting by other means by providing access to facilities and employees.

Foreign Visits: Technique

Attempts to access information or technology may occur at any time and may come from one-time visitors, long-term visitors such as exchange employees, or from frequent visitors such as foreign business associates.

Foreign Visits: Methods of Operation

The most common methods of operation used during Foreign Visits are the Exploitation of Business Activities, Exploitation of Relationships, the Exploitation of Experts, and RFI/ Solicitation.

Foreign Visits: Methods of Contact

The most common methods of contact are Foreign Visits and Personal Contact.

Foreign Visits: Targets

This method may target government facilities, cleared facilities, and commercial facilities.

Foreign Visits: Indicators

Incidents may include the use of unauthorized devices, asking for information outside the scope of the visit, or bringing cameras or video equipment into areas where photographs are not permitted.

More Examples include:

- Hidden agendas associated with the stated purpose of the visit
- Visitors/students requesting information and then growing irate upon denial
- Wandering visitors using distractions to slip away
- New visitors added to group at last minute or switching of prescreened visitors

Foreign Visits: Countermeasures

We can protect against unauthorized access by foreign visitors by doing some simple things prior to the visit. These include coordinating with DCSA, briefing hosts and escorts on approved procedures, walk the visitor route and meeting areas to identify vulnerabilities, brief all employees about the nature of the threat from the foreign visitors and restrictions on the visitors, debrief personnel in contact with visitors, and ensure visitors don’t bring recording devices into the facility.

Foreign Collection Methods: Solicitation and Seeking Employment

FIEs often attempt to develop business relationships in order to take advantage.

Solicitation and Seeking Employment: Techniques

The solicitation and seeking employment collection methods attempt to place foreign personnel in the facility with targeted information and technology. It also has foreign personnel working closely with cleared personnel so that personal relationships may be formed and possibly exploited.

Solicitation and Seeking Employment: Methods of Operation

The most common methods of operation used in an adversary seeking employment are the Exploitation of Business Activities, Resume Submission, Exploitation of Relationships, and RFI/ Solicitation.

Solicitation and Seeking Employment: Methods of Contact

The most common methods of contact are Email, Personal Contact, and the Submission of Professional Resumes.

Solicitation and Seeking Employment: Targets

FIEs using the solicitation and seeking employment collection method can participate in joint ventures or research partnerships, or internship programs for foreign students.

Solicitation and Seeking Employment: Indicators

Incidents may include foreign visitors requesting access to facilities, networks, or company personnel information, or mailing or transmitting documents to a foreign embassy or foreign country.

Solicitation and Seeking Employment: Countermeasures

We can protect against this collection method by having a TCP in place, sharing the minimum amount of information required for joint ventures or research partnerships, and educating company personnel on how to recognize and handle elicitation.

More examples include:

- Review all documents being faxed or mailed; use a translator, when necessary
- Provide foreign representatives with stand-alone computers
- Sustainment training
- Refuse to accept unnecessary foreign representatives into the facility

Foreign Collection Methods: Elicitation and Recruitment

FIE elicitation and recruitment is a covert, multiphase process.

Elicitation and Recruitment: Techniques

FIEs will spot and assess an individual for potential recruitment, cultivate a relationship with the individual, and then either elicit information or recruit the individual.

Elicitation and Recruitment: Methods of Operation

The most common methods of operation used in Elicitation and Recruitment are the Exploitation of Relationships, Exploitation of Insider Access, and the Exploitation of Security Protocols.

Elicitation and Recruitment: Methods of Contact

The most common methods of contact are Personal Contact and Social or Professional Networking.

Elicitation and Recruitment: Targets

FIEs are not necessarily looking for someone with a high level of access. Sometimes the potential for future access or the ability of the recruit to lead to other high value targets.

Trade shows, business contacts, social events, or online venues, such as chat rooms and social media, are used for this process. During the Spot and Assessment phase, the FIE will often explore potential exploitable weaknesses that can be used against the individual.

Elicitation and Recruitment: Indicators

Once a potential target has been identified, adversaries begin to cultivate a relationship with that individual that includes meeting in private so they are less likely to be observed or reported. By the time the recruitment and handling phase is initiated, the individual is likely emotionally tied to the adversary. Elicitation is the strategic use of conversation to subtly extract information about you, your work, and your colleagues. Foreign intelligence entities elicit information using both direct and indirect questioning. They may create a cover story to explain the line of questioning in their attempts to make the discussion less suspicious.

Elicitation and Recruitment: Countermeasures

Do not share anything the elicitor or recruiter is not authorized to know, including personal information about yourself, your family, or your co-workers. What can you do if you believe that someone is attempting to elicit information from you?

You can change the topic, refer them to public websites, deflect the question, provide a vague answer, or feign ignorance and ask the elicitor to explain what they know.

Knowledge Check Activity

Question 1 of 4
Which of the following are foreign collection methods?

- □ Requests for information
- □ Suspicious Network Activity
- □ Seeking employment
- □ Foreign visits
- □ Abduction and interrogation

Answer: Requests for information, suspicious network activity, seeking employment, and foreign visits are all foreign collection methods.

Question 2 of 4
Match corresponding activities with its foreign collection methods.

Foreign Collection Methods
A. Requests for Information
B. Academic Solicitation
C. Elicitation and Recruitment
D. Solicitation and seeking employment
E. Foreign visit
F. Conferences, Conventions, and Trade Shows

Activities
___ Unsolicited and direct requests often submitted via email
___ Application to degree programs associated with cleared facilities or programs
___ Involves establishing emotional relationship with the target
___ May use joint ventures or research partnerships
___ Exchange employees or foreign business associates
___ Experts may receive all-expense-paid invitations to lecture

Answer: Unsolicited and direct requests often submitted via email is an example of a request for information. Application to degree programs associated with cleared facilities or programs is an example of academic solicitation. Establishing an emotional relationship with the target is an example of elicitation and recruitment. Using joint ventures or research partnerships is an example of solicitation and seeking employment. Exchange employees or foreign business associates are an example of foreign visit. Experts may receive all-expense-paid invitations to lecture are an example of conferences, conventions, and trade shows.

Question 3 of 4
Match potential countermeasures with foreign collection methods.

List of potential countermeasures
A. Conduct audits at least weekly
B. Use mock-ups instead of actual equipment
C. Brief hosts and escorts on approved procedures
D. Share the minimum amount of information appropriate to the scope of venture

List of foreign collection methods
___ Suspicious network activities
___ Conferences, Conventions, and Trade Shows
___ Foreign Visits
___ Solicitation and Seeking Employment

Answer: Conducting audits at least weekly is a countermeasure for suspicious network activities. Using mock-ups instead of actual equipment is a countermeasure for conferences, conventions, and trade shows. Briefing hosts and escorts on approved procedures is a countermeasure for foreign visits. Sharing the minimum amount of information appropriate to the scope of venture is a countermeasure for solicitation and seeking employment.

Question 4 of 4
You decide that you need three specific types of information for the training session that you are planning. Match the information that you need with the source from which you can obtain the information:

List of Information Types

A. Trends related to what is targeted and methods used
B. Threat assessment for your current contract
C. Identify the current national security concerns that may affect your facility
D. Determine the types of crimes that are being committed at facilities close to your company

List of Source Documents

___ Federal Bureau of Investigations
___ State or Local Law Enforcement
___ DCSA CI Directorate
___ Government Contracting Agency

Answer: DCSA CI Directorate is the source where you will find trends related to what is targeted and methods used. The Government Contracting Agency is where you will find information on threat assessment for your current contract. The Federal Bureau of Investigation is the source where you can identify the current national security concerns that may affect your facility. State or local law enforcement is the course where you can find information about the types of crimes that are being committed at facilities close to your company.

Lesson Summary

You've just finished your research for today. Now, you are familiar with sources of threat information and the role of DCSA in CI and threat awareness. You should also be able to give examples of types of threats, identify employees who are vulnerable to targeting, and recognize common methods FIEs use to collect information and associated countermeasures.

DCSA resources available to industry

- DCSA CI Special Agent
- Industrial Security Representative
- Targeting U.S. Technologies Report

Sources of Threat Information for use in your CI program

- Government Contracting Agency
- DCSA CI Directorate
- FBI

- Other Federal, State, and local Agencies
- Open Sources

Types of Threats to Industry

- Insider Threats
- Threats from FIEs
- Terrorist Organizations
- Criminal Activities
- Business Competitors

Provide awareness training on foreign collection methods and associated countermeasures

- Requests for information
- Academic solicitation suspicious network activity
- Targeting at trade shows
- Seeking employment
- Foreign visits
- Elicitation

Countermeasures and Threat Reporting

Introduction to Countermeasures and Threat Reporting

There are some final elements required to finalize your CI Integration Plan. You learned about countermeasures that can be applied to each method of operation. In this lesson, we will explore detailed countermeasure efforts, and learn about the two pillars of counterintelligence programs: awareness and reporting. Please review the objectives.

Today's objectives

- Define countermeasures
- Identify employee vulnerability to targeting by foreign intelligence entities
- Identify the purpose of foreign travel and foreign visit programs
- Describe CI training requirements for industry
- Explain counterintelligence and threat information reporting requirements

Resources for today's research are located on your desktop.

Countermeasures

As we learned in the last lesson, countermeasures are the employment of devices or techniques that impair the operational effectiveness of enemy activity. Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities. The purpose of countermeasures is to adjust the behavior of potential FIEs so that they do not pose a threat to your company.

Countermeasures attempt to deter, detect, and deny access to employees, information, and technology by FIEs. Countermeasures also attempt to make the environment suitable for appropriate behavior; unsuitable for inappropriate, criminal, or terroristic behavior; and mitigate the actions of both hazards and threats.

Here are some strategies for the implementation of countermeasures in your CI awareness program.

- Train employees to recognize and report potential threats
- Control access to the target
- Deter FIEs from acting
- Degrade the process of any FIE into or out of the facility
- Respond to any active threat situation
- Create an environment where people feel safe and secure and can focus on the company's goals
- Design programs to mitigate possible harm from hazards and FIEs

Employee Vulnerability to Targeting by Foreign Intelligence Entities

Your employees must understand that a single piece of information - classified or not- may not be of critical importance alone, but when put together with other pieces of information, may reveal sensitive, or even classified, information. For this reason, employees need to protect not

only classified information, but also controlled unclassified information, business proprietary information, and intellectual property. The loss of any of these directly impacts your company's economic viability and potentially the nation's security.

We need to know who these employee groups are, so you can make them aware of potential contact from adversaries. The better prepared they are, the lower the chance of compromising your facility's sensitive information. Some groups are more vulnerable to targeting than others. These groups include human resources, information technology, business development, research and development, manufacturing, purchasing, facility management, and employees traveling abroad.

Let's talk about each of these groups individually.

Human Resources

Human resources personnel are the gateway to your facility. They are appealing targets for adversaries because of their access to personnel information and because they play an important role in the hiring process. HR personnel can be an important part of your CI program. Their access to personnel information equips them to recognize targeting via academic solicitation and seeking employment.

Information Technology

IT personnel are the electronic gatekeepers for your facility. They are appealing targets for adversaries because of their access to the facility's network and information systems where critical information resides. IT personnel can be central to your CI program. Their access to system and network activity equips them to notice anomalies and spot cyber attacks.

Business Development

Business development personnel are appealing targets because of their access to your sensitive and proprietary information and because they play a key role in determining with whom you do business. Business development personnel are important to your CI program. Their access to the people seeking to do business with your company enables them to help identify potential targeting early and identify what is being targeted.

Research and Development

Engineers and research and development personnel are targets due to their knowledge of and access to critical technology assets including blueprints, diagrams, and other technical information. This group can identify specific information being targeted based on the inquiries and solicitations they receive.

Manufacturing

Manufacturing and direct labor personnel are targets because of their access to the facility and its technology, processes, and end products. This group can identify specific assets being targeted and help identify methods of operations used.

Purchasing

Individuals working in purchasing are targets because of their access to the company's supply chain. Purchasing personnel can support the CI Program by identifying and reporting suspicious interactions with vendors.

Facility Management

Facilities management personnel are appealing targets because of their physical access to your facility and all of the information, technology, and personnel within it. This group is also an asset to the CI Program because they are uniquely positioned to observe the movement in, out, and between facilities by employees and visitors.

Employees traveling abroad

Employees have access to sensitive company information and are targeted for this information when they travel abroad or when they represent your company at trade shows, conventions, and seminars. You must educate all employees on the risks associated with foreign travel and provide them with a foreign travel briefing before they go to increase their awareness of potential targeting and to provide information on current travel warnings and alerts.

When an employee returns from foreign travel, you must conduct a foreign travel debrief. This is an opportunity to gather information and determine if your personnel were targeted and if so, how they were targeted. Information indicative of targeting should be reported as a suspicious contact. It can also provide information that helps you prepare for future travel.

Employees participating in trade shows, conventions and seminars should also be briefed prior to and after attending such events to increase awareness of risk and encourage reporting of suspicious activity.

You can learn specific information about CI foreign travel briefings in the DCSA web-based training Short CI Foreign Travel Briefing.

Foreign Travel

As discussed, though employees may be targeted at any time or place, FIEs have greater access to employees during foreign travel and employees are most vulnerable during transit. Organizations should establish a Foreign Travel Program and standard operating procedures that require employees to report both official and personal foreign travel. The purpose of a Foreign Travel Program is to prepare travelers for events they may encounter and arm them with the strategies needed to handle these events.

FSOs should provide education briefings prior to travel and require employees to participate in a security debrief upon completion of foreign travel. Foreign travel briefings increase the traveler's awareness of potential targeting by FIEs and personal safety needs while traveling internationally, provides information on current travel warnings and alerts, and provides travelers information about where to seek assistance while traveling abroad.

When personnel return from foreign travel, you will conduct a debrief session with them. The purpose of the debrief is to determine if anything happened during the trip that raises concern for the traveler or for the organization. Depending upon the purpose and destination of the travel, this debrief can be as informal as a questionnaire or as formal as an interview.

Foreign Travel Debriefing may cover:

- Countries and dates visited
- Irregularities at port of entry
- Gifts or provisions received
- Foreign inquiries
- Requests received
- Unexpected or unusual events
- Suspicious foreign contacts
- Other info

Foreign Visits

International visits with cleared contractors are a common part of everyday business in today's global economy. We must acknowledge the associated potential counterintelligence vulnerabilities to ensure that the requirements of the National Industrial Security Program Operating Manual or NISPOM are followed.

Inform your DCSA industrial security representative or DCSA CI agent in advance of foreign visits. Given adequate time, your agent can assist with identifying the risk to the cleared company.

Establish a Technology Control Plan, or TCP, that identifies procedures for restrictions of any Foreign Liaison Officers or long-term visitors with access to the facility.

When a foreign visit occurs at your facility, awareness is essential to prevention.

Watch for wandering visitors, questions that are not associated with the purpose of the visit, visitors asking the same question of multiple contractors, visitors switching agenda topics or questions or visitors becoming distraught when irregular questions are not answered.

Remember that even if an appropriate authority grants a foreign visitor access to classified U.S. information, that visitor is NOT entitled to classified information unless he/she has a direct need to know that has been communicated and verified in advance of the visit.

Here are some elements of an effective foreign visit program.

- Pre-visit: Education program for escorts, briefers, and hosts that educates on responsibilities
- Post-visit: Debriefing program that solicits responses from escorts, briefers, and hosts on reportable incidents
- Verification of visitors' identities
- Identification and reporting of anomalies related to foreign visits

- TCP includes procedures for restrictions of any Foreign Liaison Officers or long-term visitors with access to the facility

CI Training

NISPOM requires contractors to provide all cleared employees with security training and briefings commensurate with their involvement with classified information to include initial and annual refresher training. NISPOM requires contractors to establish internal procedures to ensure that cleared employees are aware of their responsibilities for reporting pertinent information.

FSOs must use facility standard operating procedures or SOPs, initial, and recurring training to ensure that employees are aware of and follow reporting procedures. Your company should also establish standard operating procedures to address responsibilities and company requirements.

DCSA and the Cognizant Security Agency or CSA provide defensive security, threat awareness, and other education and training information for contractors to use in their CI awareness training.

As an FSO, you are responsible for providing CI and threat awareness training at your facility. Engaging in certain activities, on a regular basis, will help you do this effectively.

First, you must adhere to initial and annual training requirements. Ensuring employees receive security and CI training helps protect your facility and national security. But having an effective CI awareness program involves more than just annual CI briefings.

You should implement an ongoing campaign to help employees maintain vigilance against the threat posed by FIEs. This “vigilance campaign” should be tailored for situations common to your company employees, use a variety of communication methods, highlight key CI concepts, and reinforce reporting requirements and points of contact.

You can be creative in selecting ways to enhance messaging and awareness. Monthly activities such as contests to create a new awareness poster, playing CI Awareness Trivial Twirl, or watching relevant videos will engage employees and stimulate their awareness.

You can establish a CI awareness week and have guest speakers from DCSA or other agencies to provide updates on current threats and methods, have company leadership emphasize company SOPs, and provide informational briefings.

Placing visual reminders prominently throughout the facility is another way to promote awareness. Posters from your monthly contest and from DCSA, flyers for offices or cubicles and short reminders on post-its are ways to keep CI awareness in front of employees.

You can also use your company’s website and social media such as the company’s Facebook or Twitter to send out short awareness messages.

CDSE’s Counterintelligence Toolkit has resources that can be used to help develop a “Vigilance” mindset within your company.

Finally, you must maintain records of training provided and employee participation. This requirement may be satisfied by use of distribution lists, facility or department-wide newsletters, or other means identified in your company SOPs.

Reporting Requirements

Your personnel are the first line of defense against threats. Everyone must be vigilant and report any incident or behavior that may relate to a potential compromise of sensitive unclassified or classified information.

So, what must be reported and to whom? The NISPOM requires employees of cleared industry to report events that impact the status of the facility clearance, impact the status of an employee's personnel security clearance, affect proper safeguarding of classified information, or indicates that classified information was lost or compromised. These threats are reported to the FSO.

Depending on the situation, FSOs must report the possible threat to the DCSA which is the CSA, via your DCSA Industrial Security Representative, or DCSA Counterintelligence Special Agent.

FSOs are required to report information concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities to the FBI and DCSA. Initial reports to the FBI can be made by phone but must be followed up with a written report. Remember that although espionage reports go immediately to the FBI, the DCSA (or the CSA) must also be informed.

Security Violation: Failure to comply with the policy and procedures established by this Manual that reasonably could result in the loss or compromise of classified information.

Reporting Requirements (cont.)

NISPOM 1-300 requires contractors to establish internal procedures to ensure that cleared employees are aware of their responsibilities for reporting pertinent information. FSOs must use facility standard operating procedures, a threat vigilance campaign, and training to ensure that employees are aware of and follow reporting procedures. FSOs must use their vigilance campaign, recurring training, and travel briefings to stress how critical it is for everyone in the facility to report all suspicious activity or contacts they observe.

It is important for employees to know that reporting does not reflect negatively on their facility. In fact, DCSA expects companies, especially those in certain industries, to report suspicious activity, and to report often!

The best way to defeat the threat is to report the threat. Reporting helps to identify the larger threat across cleared facilities and enables industry to use that information to develop countermeasures.

The reporting process works like this. When our facility submits a report, DCSA evaluates, screens, and analyzes it. By analyzing all of the reports gathered from industry over time, DCSA is able to develop current, specific threat information. DCSA then provides this consolidated information back to industry, which better equips companies to develop appropriate countermeasures to address new and emerging threats.

Adverse Information: Adjudicative Guidelines

NISPOM 1-302a requires contractors to report any adverse information relating to cleared employees to DCSA. Adverse information is any information that negatively reflects on the integrity or character of a cleared employee, that suggests a cleared employee's ability to safeguard classified information may be impaired, or that a cleared employee's access to classified information clearly may not be in the interest of national security.

Adverse information may impact the status of a cleared employee's personnel security clearance and is evaluated according to the 13 adjudicative guidelines contained in Security Executive Agent Directive 4 or SEAD 4. This directive establishes the common adjudicative criteria for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

We must report any information regarding your own or others' behavior that is not consistent with, or that violates, the 13 adjudicative guidelines.

- Guideline A: Allegiance to the United States
- Guideline B: Foreign Influence
- Guideline C: Foreign Preference
- Guideline D: Sexual Behavior
- Guideline E: Personal Conduct
- Guideline F: Financial Considerations
- Guideline G: Alcohol Consumption
- Guideline H: Drug Involvement and Substance Misuse
- Guideline I: Psychological Conditions
- Guideline J: Criminal Conduct
- Guideline K: Handling Protected Information
- Guideline L: Outside Activities
- Guideline M: Use of Information Technology

The behaviors identified in the 13 adjudicative guidelines raise doubts about an individual's reliability, trustworthiness, and judgment in protecting national security.

Reportable Adverse Information

Now, let's consider specific incidents that must be reported. These include mishandling classified information, misuse of computer systems, suspicious cyber incidents, foreign influence, suspicious contacts, suspicious financial activities, and the unauthorized use of recording devices. Take a moment to review examples of these incidents. Remember, you might encounter signs or actions not listed here. When in doubt, always err on the side of caution and report the incident.

Mishandling Classified Information

Mishandling classified information includes attempting to gain access to classified information without a need to know, unauthorized removal, copying, or transmittal of classified information.

Examples include:

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

Misuse of Computer Systems

Misuse of computer systems includes unauthorized access to classified networks or files, attempts to access someone's login credentials, data spills, unauthorized data transmission, and any introduction of unauthorized elements into information systems.

Examples include:

- Unauthorized network access
- Unauthorized email traffic to foreign destinations
- Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading
- Use of DoD account credentials by unauthorized parties
- Unexplained storage of encrypted data
- Network spillage incidents or information compromise
- Unauthorized transmissions of classified or controlled unclassified information
- Data exported to unauthorized domains affecting classified information, systems or cleared individuals
- Actual or attempted unauthorized access into U.S. automated information systems
- Tampering with or introducing unauthorized elements into information systems
- Unexplained user accounts, administrator accounts, and expansion of network privileges

Suspicious Cyber Incidents

Suspicious cyber incidents involve malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers or engineering, electronic elicitation, email spoofing, spear phishing, whale phishing, or direct questioning, such as through social networking sites.

Examples include:

- Advanced techniques and/or advanced evasion techniques, which imply a sophisticated adversary
- Pre-intrusion aggressive port scanning
- Denial-of-service attacks or suspicious network communication failures

- Social engineering, electronic elicitation, email spoofing, spear phishing, whale phishing, or direct questioning, such as through social networking sites
- Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration
- Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage
- Any cyber activity linked to law enforcement or counterintelligence suspicious indicators provided by the FBI, DCSA, Defense Intelligence Agency or by any other cyber centers

Foreign Influence

Foreign influence might involve unreported close and continuing contact with a foreign national, including intimate contacts, shared living quarters, or marriage.

Examples include:

- Undisclosed visits to foreign diplomatic facilities
- Trips to foreign countries inconsistent with an individual's financial ability
- Foreign entities targeting employees traveling overseas via airport screening or hotel room incursions

Suspicious Contacts

NISPOM defines suspicious contacts as efforts by any person, regardless of their nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee, contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests a cleared employee may be the target of an attempted exploitation by an FIE.

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

Suspicious Financial Activity

Concerning financial activity might include unexplained expensive purchases not reasonably supported by the individual's income or sudden unexplained reversal of a negative financial situation or repayment of large debts.

Unauthorized use of Recording Devices

The unauthorized possession of cameras or recording or communication devices in classified areas or the discovery of suspected surveillance devices in classified areas.

Reporting Suspected Activity

Hey there. I just dropped by to see how you're coming along with preparing your CI Integration Plan. Oh, I see that you were just researching reporting requirements. If you have a few minutes, we can talk about a few hypothetical incidents and how the employees should respond.

Situation 1

Frank is an Aircraft Technical Data Controller. Last year, Frank supported a multi- national airshow where his company's newest aircraft was showcased. Frank was responsible for giving foreign pilots a "walk-around" of his company's aircraft.

After the airshow, one of the foreign pilots ran into Frank in the hotel lounge where they talked and watched a game together. Frank and the foreign pilot met for drinks at a tavern down the street from the hotel each evening for the remainder of the week until the air show was over.

Later, Frank was overheard discussing a free two-week vacation at the Khyber Himalayan Resort & Spa in the Himalayas with the foreign pilot. A few weeks later, Frank mentioned that his foreign pilot friend's overseas bank is securing his loan to purchase a timeshare in the Outer Banks.

Does this situation contain reportable activities or behavior?

- o Yes
- o No

Answer: This is definitely reportable behavior. There are actually three separate reportable events in this situation. Frank should have reported the social event with foreign contact, the coworkers should have reported the expensive, free vacation to a resort, and the coworkers should have reported the timeshare purchase using a foreign bank. Frank actually reported the situation to his FSO, who in turn notified the facility's DCSA CI Agent.

Situation 2

During the monthly audit of the computers at your Seattle location, keystroke logging software was found loaded on computers in three separate work centers that handle classified technology. The login credentials of a single company employee were found to have been used to access each of the computers.

Does this situation contain reportable activities or behavior?

- o Yes
- o No

Answer: Yes. This incident should be reported to both the FBI and DCSA. This incident was actually reported. It represents not only potential information collection and transmittal, but potential espionage.

Situation 3

Ian works in the Logistics department and has recently changed his work hours and started bringing a backpack to work. He comes to work half an hour before his scheduled start time and spends time talking with two individuals in the Research and Development department. He was observed putting a document in his backpack while in the R&D department one day.

Does this situation contain reportable activities or behavior?

- o Yes
- o No

Answer: Yes. This is suspicious behavior and the event was reported to the FSO. The FSO investigated and determined that Ian had started a new exercise routine. He was going to the R&D employees for advice on his weightlifting workouts. The documents Ian was observed putting into his backpack were actually his workout logs. It is refreshing to see that not everything that appears suspicious is an attempt to gain access to sensitive or classified information.

Situation 4

Your company advertised a paid six-month internship in the engineering department. A foreign exchange student responded to the advertisement but her area of study in the U.S. was economics and she did not have the minimum required knowledge or skills for the internship.

When we did not select her for an interview, she contacted HR by phone and offered to work without compensation under the internship. A week later, she came to the facility and tried to speak with "the person in charge of the internship."

Does this situation contain reportable activities or behavior?

- o Yes
- o No

Answer: Yes. This is suspicious behavior and the event was reported to the FSO. Since this was a cleared facility, the person could have been attempting to gain access in order to collect information. This event was reported to DCSA.

Situation 5

The Research and Development department had an unannounced visit from two men representing themselves as working for a company that wanted to establish a joint venture. They asked for a tour of your facility to determine if your research capability and quality standards were sufficient for them to accept as a partner. We, of course, refused to give them a tour, took their business cards, and notified the Business Development department. When Business Development attempted to contact the company, the phone number was to a person's residence who knew nothing about the business.

Does this situation contain reportable activities or behavior?

- o Yes
- o No

Answer: Yes. While it is not clear that the visitors were foreign, their behavior was certainly suspicious. Remember, suspicious activity of ANY persons must be reported. No foreign connection is required. This event requires reporting to DCSA under NISPOM 1-302b.

Knowledge Check Activity 1

Question 1 of 4

Which of the following activities can you use to promote CI awareness within your facility?

- □ Enlist your DCSA CI Special Agent to brief employees
- □ Post CI-related material throughout the workplace
- □ Share actual targeting examples with employees
- □ Remind employees that anyone who appears "foreign" is a threat

Answer: We can promote CI awareness within your facility by enlisting your DCSA CI Special Agent to brief employees, post CI-related material throughout the workplace, and share actual targeting examples with employees.

Question 2 of 4

Foreign travel increases the risk of FIE targeting.

- o True
- o False

Answer: True. Although employees may be targeted at any time or any place, FIEs have greater access to employees during foreign travel.

Question 3 of 4

The National Industrial Security Program Operating Manual (NISPOM) requires employees of cleared industry to report which of the following events?

- □ Suspicious contacts
- □ Lost or compromised classified information
- □ Actions/events that may affect the status of an employee's personnel security clearance
- □ Actions/events that may affect the status of the facility's clearance
- □ Actual, probable, or possible espionage, sabotage, terrorism, of subversive activities

Answer: NISPOM requires employees of cleared industry to report suspicious contacts lost or compromised classified information, actions or events that may affect the status of an employee's personnel security clearance, actions or events that may affect the status of the facility's clearance, and actual, probable, or possible espionage, sabotage, terrorism, of subversive activities.

Question 4 of 4

Which of the following groups are vulnerable to foreign intelligence entity targeting?

- □ Information technology
- □ Facility management
- □ Employees traveling abroad
- □ Administrative assistants Knowledge Check Screen 3 of 4

Answer: Information technology, facility management, employees traveling abroad and administrative assistants are all groups vulnerable to foreign intelligence entity targeting.

Knowledge Check Activity 2

Question: You learn from a security bulletin that a foreign country is using university students applying for low level jobs to gain entry into companies in your industry. Which group might you alert first?

- Human Resources
- Information Technology
- Business Development
- Engineers and Research & Development

Answer: You would alert Human Resources when a foreign country is using university students applying for low level jobs to gain entry into companies in your industry.

Question: Foreign entities stepped up attempts to purchase export-controlled technology, including technology your facility develops. Who should you alert?

- Human Resources
- Information Technology
- Business Development
- Engineers and Research & Development

Answer: You would alert Business Development when foreign entities step up attempts to purchase export-controlled technology, including technology your facility develops.

Question: You learn of a threat from a business competitor to steal blueprints and schematics. Which group might you alert first?

- Human Resources
- Information Technology
- Business Development
- Engineers and Research & Development

Answer: You would alert Engineers or the R&D when you learn of a threat from a business competitor to steal blueprints and schematics.

Question: There is an increase in cyber-attacks against companies in your industry. Who should you alert?

- Human Resources
- Information Technology
- Business Development
- Engineers and Research & Development

Answer: You would alert IT when there is an increase in cyber-attacks against companies in your industry.

Lesson Summary

Well, this completes your final training session. The technology and information created, maintained, and updated by cleared industry is under constant threat from FIEs seeking to gain military, economic, and technological advantage. Remember, timely and accurate reporting from cleared contractors, such as your company, is the primary tool DCSA uses to identify and mitigate collection efforts targeting information and technology resident at cleared facilities.

Today's objectives

- Defined countermeasures
- Identify employee vulnerability to targeting by foreign intelligence entities
- Identified the purpose of foreign travel and foreign visit programs
- Described CI training requirements for industry
- Explained counterintelligence and threat information reporting requirements

Let's have a look at what information you have collected for your CI Integration Plan.

Use strategies for implementing countermeasures

- Train employees to recognize and report potential threats
- Control access to the target
- Deter FIEs from acting
- Delay the progress of any FIE into or out of the facility
- Respond to any active threat action
- Gather evidence for prosecution, investigations, and training
- Create an environment where people feel safe and secure and can focus on the company's goals
- Design programs to mitigate possible harm from hazards and FIEs

Establish a Foreign Travel Program

- Conduct foreign travel pre-briefings
  - Vulnerability awareness
  - Personal safety
  - Terrorist threat
  - Assistance contacts
- Conduct foreign travel debriefings
  - Countries and dates visited
  - Irregularities at port of entry
  - Gifts or provisions received
  - Foreign inquiries
  - Requests received
  - Unexpected or unusual events
  - Suspicious foreign contacts

Establish a Foreign Travel Program (cont.)

- Notify DCSA CI Agent of visit

- Verify visitors' identities
- Conduct pre-visit awareness briefings
- Designate visitor escorts
- Conduct post-visit debriefings

Conduct CI Training

- Follow NISPOM initial and annual training requirements
- Publicize company SOPs relating to CI
- Incorporate DCSA resources from the Counterintelligence Toolkit into training
- Establish a CI vigilance campaign and include such items as:
  - Weekly awareness
  - Monthly activities
  - Visual awareness reminders
  - Include social media

Reporting

- Publicize reporting requirements
  - Give examples of reportable events

Practical Exercise

Practical Exercise Introduction

You're filling in for the FSO, your duties are to answer security questions and provide guidance.

Practical Exercise Question 1

Hey there! I just have a quick question for you. I know that we have to report threats, but I am unsure what the role of CI is in threat awareness.

What is the role of reporting in counterintelligence and threat awareness?
How should you respond to Michael?

Select all that apply.

- □ Reporting is a form of self-monitoring that reduces the need of Government inspections at your facility.
- □ Reporting helps to disrupt foreign collection activity.
- □ Reporting identifies threats so that countermeasures can be developed.
- □ Reporting eliminates all risk.

Answer: Reporting helps to disrupt foreign collection activity and to identify threats so that countermeasures can be developed.

Practical Exercise Question 2

When Denise approached and greeted Charles, she noticed that he was discussing a component that they are developing and had actually sketched the component on a napkin. Charles and Denise work for a cleared contractor but their project is not classified.

Should this event be reported?

- o Yes
- o No

Answer: This event should be reported because a single piece of information - classified or not - may not be of critical importance alone, but when put together with other pieces of information, may reveal sensitive, or even classified, information.

Practical Exercise Question 3

Hello. This is Victor from Facilities Management. I'm in the Engineering Department. None of the engineers are here and the classified storage container is open. It's not just unlocked; the drawer is pulled out and there are several folders visible.

To whom should you report this incident?

- □ FSO
- □ FBI
- □ DCSA

- □ Local Law Enforcement

Answer: NISPOM 1-301 requires employees of cleared industry to report all events that indicate classified information may have been compromised to the FSO, FBI and Cognizant Security Authority (DCSA for industry).

Practical Exercise Question 4

Hello there. I am just returning from a trip to Turkey. So, I know that I need to schedule a debriefing with you but, something happened, and I want to know if I need to report it. While I was at the airport waiting for my return flight, a woman approached me and started a conversation about social media and how it allows women to share their successes. When the woman learned that I have a Twitter account, she wanted to know who I was so that she could follow me. The woman asked if I could tweet about the company I work for, what I do, and who my coworkers are. I told her that I had to go and didn't give her my Twitter handle.

Should this event be reported?

- o Yes
- o No

Answer: This event should be reported. Although this could have been a person being friendly, the request to tweet about coworkers sounds suspicious.

Course Conclusion

Meeting with Company CEO

Good morning. I was happy to get your message that you have a draft for the CI Integration Plan for me to review. Let's have a look at it.

Well, that is a good start. Let's get together with senior leadership on Thursday and discuss this plan. We can determine if this timeline will work across departments and make some assignments. Although we will depend on you as the FSO heavily, you can't make this work alone.

All of our senior leadership and key personnel from departments need to take some responsibility for integrating CI and threat awareness into our security program.

Course Summary

Incorporating counterintelligence or CI and threat awareness into your security program makes our program stronger and more successful.

Now, you should be able to recognize types of threats, common methods used to collect information, collection indicators and countermeasures, how the analytical risk management process can be used in risk mitigation, identification of threats, sources of threat information, and reporting requirements.

This knowledge will enable you to protect our company and its valuable assets, and in turn, the national security of the United States. Remember to look at the course resources before you go. There are several job aids that you may be able to use at your facility.

Objectives:

- Identified the purpose of incorporating CI and threat information into a security program.
- Identified CI and threat awareness policy requirements for industry and DoD personnel.
- Identified the role of DCSA Counterintelligence Directorate in CI and threat awareness.
- Gave examples of types of threats
- Identified employee vulnerability to targeting by foreign intelligence entities.
- Recognized common methods of operation used for collecting information.
- Explained the role of analytical risk management in risk mitigation
- Identified key sources of threat information.
- Explained counterintelligence and threat information reporting requirements and procedures

Conclusion

Congratulations! You have completed the Protecting Assets in the NISP Course.