Student Guide

Establishing an Insider Threat Program for Your Organization

Course Introduction

Course Introduction

Course Overview

Threats from insiders are serious and they are happening now. You and your organization are at risk. You already know what an insider threat is… but what can you do to combat it? As a security manager, what must you do?

Welcome to the Establishing an Insider Threat Program for Your Organization course.

Course Objectives

In this course you will learn about establishing an insider threat program and the role that it plays in protecting you, your organization, and the nation. You will learn the policies and standards that inform insider threat programs and the standards and strategies you will use to establish a program within your organization.

Here are the course objectives. Take a moment to review them.

- Identify the policies and standards that inform the establishment of an insider threat program
- Identify key challenges to detecting the insider threat
- Identify key steps to establishing an insider threat program
- Identify the minimum standards for implementing an insider threat program
- Identify program strategies for:
    - Monitoring user activity on classified networks
    - Evaluating personnel security information
    - Training cleared employees on the insider threat

Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 1: Insider Threat Program Requirement

Introduction

Objectives

Who could become an insider threat? An insider is any person with authorized access to any United States government resource, such as personnel, facilities, information, equipment, networks or systems. An insider threat refers to an insider who wittingly or unwittingly does harm to the security of the United States. This threat can include espionage, terrorism, sabotage, unauthorized disclosure of national security information, or the loss or degradation of departmental resources or capabilities. Insider threat programs seek to mitigate the risk of insider threats.

This lesson will review program policies and standards. It will also discuss the key challenges to detecting insider threats.

Regulatory Framework

Background

We are all too familiar with the most notorious of insider threat cases. In response to the threat from insiders, national policy issued in late 2011 requires government agencies to establish insider threat programs. For now, this policy applies only to classified information, though its principles can help you protect all of your organization's information. Let's take a closer look at the policy and its requirements.

National Policy

Executive Order 13587 establishes the requirement for government agencies to establish their own insider threat programs. The Order defines the insider threat program purpose as deterring, detecting, and mitigating insider threats.

Insider threat programs are intended to: Deter cleared employees from becoming insider threats; detect insiders who pose a risk to classified information; and mitigate the risks through administrative, investigative, and other response actions.

The Executive Order also includes general department and agency responsibilities that we will discuss throughout this course.

General Department and Agency Responsibilities

- Within 180 days of the effective date of this policy (May 20, 2013), establish a program for deterring, detecting, and mitigating insider threat; leveraging counterintelligence (CI), security, information assurance, and other relevant functions and resources to identify and counter the insider threat.

- Establish a centralized capability to monitor, audit, gather and analyze information for insider threat detection and mitigation. Critical program requirements include but are not limited to: (1) monitoring user activity on classified computer networks controlled by the Federal Government; (2) evaluation of personnel security information; (3) employee awareness training of the insider threat and employees' reporting responsibilities; and (4) information analysis, reporting, and response capability.

- Develop and implement sharing policies and procedures whereby the organization's insider threat program accesses, shares, and integrates information and data derived from offices across the organization, including CI, security, information assurance, and human resources offices.

- Designate a senior official(s) with authority to provide management, accountability, and oversight of the organization's insider threat program and make resource recommendations to the appropriate agency official.

- Consult with records management, legal counsel, and civil liberties and privacy officials to ensure any legal, privacy, civil rights, civil liberties issues (including use of personally identifiable information) are appropriately addressed.

- Promulgate additional department/agency guidance, if needed, to reflect unique mission requirements but not inhibit meeting the minimum standards issued by the Insider Threat Task Force (ITTF) pursuant to this policy.
- Perform self-assessments of compliance with insider threat policies and standards; the results of which shall be reported to the Senior Information Sharing and Safeguarding Steering Committee (hereinafter Steering Committee).
- Enable independent assessments, in accordance with Section 2.1(d) of EO 13587, of compliance with established insider threat policy and standards by providing information and access to personnel of the Insider Threat Task Force (ITTF).

Minimum Standards

In November 2012, the Executive Branch issued Minimum Standards for Executive Branch Insider Threat Programs. Issued in the form of a Presidential Memorandum, these standards outline the minimum requirements to which all executive branch agencies must adhere. These elements include the capability to gather, integrate, centrally analyze, and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel.

While the Minimum Standards provide the minimum elements needed for agencies to establish effective insider threat programs, agencies may go farther, if they choose.

Throughout this course, we will examine these minimum requirements in greater detail.

Challenges to Detecting the Insider Threat

Why Do Insiders Go Undetected?

The reason why the Executive Branch issued the insider threat national policy and minimum standards is that it is often difficult to identify insiders who pose a threat and to detect what they are doing in time to prevent harm. Insiders can operate over an extended period of time. Employees may not be trained to recognize reportable suspicious activity or may not know how to report, and even when employees do recognize suspicious behaviors, they may be reluctant to report their co-workers. It is also important to note that the unwitting insider threat can be as much a threat as the malicious insider threat. Traditional access controls don’t help – insiders already have access. Insiders can collect data from multiple systems and can tamper with logs and other audit controls. It is difficult to distinguish malicious from legitimate transactions.

Insider threat program requirements are designed to help address these challenges.

Review Activity 1

The minimum standards for establishing an insider threat program include which of the following?

Select the best responses.

- □ Establish capability to manage threat information
- □ Monitor employee classified network use
- □ Provide employee training
- □ Protect civil liberties and privacy

Review Activity 2

What is an insider threat?

Select the best response.

- ○ An insider threat is a threat that a person with access to any United States government resources will use his or her access to wittingly do harm to the security of the U.S.
- ○ An insider threat is a threat that a person with authorized access to any United States government resources will use his or her access, wittingly or unwittingly, to do harm to the security of the U.S.

Answer Key

Review Activity 1

The minimum standards for establishing an insider threat program include which of the following?

Select the best responses.

☑ Establish capability to manage threat information

☑ Monitor employee classified network use

☑ Provide employee training

☑ Protect civil liberties and privacy

All of these are included in the minimum standards for establishing an insider threat program.

Review Activity 2

What is an insider threat?

Select the best response.

○ An insider threat is a threat that a person with access to any United States government resources will use his or her access to wittingly do harm to the security of the U.S.

⊙ An insider threat is a threat that a person with authorized access to any United States government resources will use his or her access, wittingly or unwittingly, to do harm to the security of the U.S.

It is important to remember that insider threats can be both witting and unwitting.

Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 2: Setting Up an Insider Threat Program

Introduction

Objectives

Insider threat programs as outlined in the national policy and Minimum Standards seek to mitigate the risk of insider threats. This lesson provides guidance on how to set up an insider threat program in your agency or organization.

Program Establishment

Roles and Responsibilities

Each agency must establish its own capability to deter, detect, and respond to the insider threat. This centralized capability relies on several entities. There is a Senior Official who manages the program. In addition, in order to establish the program, key organization stakeholders must be involved. This can be thought of as a working group. Finally, establishing the program also includes putting in place the capability to execute the program. For ease of discussion, we'll describe this as the “hub”.

The Senior Official

The Minimum Standards require an agency to designate a Senior Official. The Senior Official plays a vital role in establishing the process of gathering, integrating, analyzing, and responding to potential insider threat information.

When establishing your own insider threat program, it is important to have the buy-in and continuing involvement of your agency's Senior Official. The Senior Official is responsible for managing and overseeing the program and providing resource recommendations to the agency head, submitting the implementation plan and annual reports to the agency head, ensuring proper handling and use of records, consulting with the Office of the General Counsel, civil liberties, and privacy officials; establishing guidelines for record retention; and facilitating oversight reviews to ensure compliance with policy.

Establishing the Working Group

When establishing your agency or organization's capability to deter, detect, and respond to the insider threat, you should establish a working group that includes representatives from key stakeholder offices within your organization. This includes those who can provide personnel-related information, such as counterintelligence, security, and human resources; those who can provide system monitoring, such as information technology and information assurance; those who can provide legal guidance, such as the office of the General Counsel; and, finally, those who can provide response capabilities, such as the Inspector General and law enforcement.

Identifying What Requires Protection

One of the key activities when establishing an insider threat program is to identify and prioritize what requires protection. This may include people, facilities, technology, equipment, and information. However, with limited resources, you cannot protect all assets. Of the assets you do protect, you cannot protect them at the same level.

To help in identifying and prioritizing, ask:

- Is the asset essential for the organization to accomplish its mission?
- Would loss of access to the asset disrupt time-sensitive processes?
- Would compromise or degradation of the asset damage U.S. national or economic security?
- Could an adversary exploit or manipulate this asset to harm the organization, U.S., or allied interests?
- Would an adversary gain advantage by acquiring, compromising, or disrupting the asset?

The answers to these questions will guide you to identify and prioritize what requires protection.

Other Considerations

When establishing the program, other considerations include:

- Who are our key agency stakeholders?
- What resources are available to us?
- What capabilities do we already have in place?
- How should we incorporate subordinate entities?
- How will we apply our program to contractors?

The answers to these questions will guide you in setting up an insider threat program within your organization.

Executing Program Capabilities

Once the insider threat program is established in your organization, there needs to be a centralized capability in place to execute the program. This centralized capability can be thought of as a hub.

Hub activities include:

- Accessing agency-internal information to detect and/or analyze potential insider threats.
- Receiving insider threat reports from inside the agency.
- Developing informed responses to insider threat activity.

Review Activity

Which of the following stakeholders should be involved in establishing an insider threat program in an agency?

Select all that apply.

□ Information Assurance

□ Security

□ Human Resources

□ Research and Development

Answer Key

Review Activity

Which of the following stakeholders should be involved in establishing an insider threat program in an agency?

Select all that apply.

☑ Information Assurance
☑ Security
☑ Human Resources
□ Research and Development

Information Assurance, Security, and Human Resources are just a few of the stakeholders that should be included.

Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 3: Minimum Standards for an Insider Threat Program

Introduction

Objectives

In this lesson, you will learn about the Minimum Standards for implementing an insider threat program.

Minimum Standards

Core Requirements

How do you develop an insider threat program?

The Minimum Standards contain the core requirements you must fulfill. They center on establishing your program's capability to analyze and respond to evidence of a potential insider threat. You must establish your program's ability to gather, integrate, review, assess, and respond to information derived from a variety of sources. You must also establish procedures for insider threat response actions to both clarify and resolve insider threat matters and to ensure that such response actions are centrally managed. Finally, you must develop procedures to document insider threat matters reported to the program and the response actions taken. These procedures must also ensure timely resolution of matters.

You will learn more about these core requirements throughout this course.

Information collection and analysis sources include:

- Counterintelligence
- Security
- Human resources
- Law enforcement
- User activity monitoring

Response procedures include:

- Threat matter clarification
- Central management of response actions

Documentation and resolution procedures include:

- Reported threats and response actions
- Timely resolution of matters

Ensure Program Access to Information

In order for your program to have any effect against the insider threat, information must be shared across your organization. As part of your insider threat program, you must direct all relevant organizational components to securely provide program personnel with the information needed to identify, analyze, and resolve insider threat matters. You must establish procedures for program requests to access sensitive information, such as special access programs. Ensuring such information will be adequately protected will facilitate cooperation by components.

The Minimum Standards also direct you to establish guidelines for reporting information to the program. This will help individuals understand what and how to report.

Finally, as part of establishing an insider threat program, you must ensure timely access to available intelligence and counterintelligence threat-related information.

You will learn more about these requirements later in this course.

Establish User Activity Monitoring Capability

The Minimum Standards require you to develop a user activity monitoring capability for your organization’s classified networks. When establishing your organization’s user activity monitoring capability, you will need to establish policies and procedures that determine the scope of the effort. Once the agency determines the recommended actions, the agency may need to allow for another agency, such as the Defense Information Systems Agency, or DISA, to provide the monitoring capability. You will need to execute interagency Service Level Agreements, where appropriate.

You will learn more about these requirements later in this course.

Personnel Training

The Minimum Standards require training for both insider threat program personnel and for cleared employees of your organization. The Minimum Standards designate specific areas in which insider threat program personnel must receive training. In addition, all cleared employees must receive training in insider threat awareness and reporting procedures.

You will learn more about these requirements later in this course.

Review Activity

When you establish your organization's insider threat program, which of the following do the Minimum Standards require you to include?

Select all that apply.

- □ Ensure access to insider threat-related information
- □ Establish analysis and response capabilities
- □ Establish user monitoring on classified networks
- □ Ensure personnel are trained

Answer Key

Review Activity

When you establish your organization's insider threat program, which of the following do the Minimum Standards require you to include?

Select all that apply.

- ☑ Ensure access to insider threat-related information
- ☑ Establish analysis and response capabilities
- ☑ Establish user monitoring on classified networks
- ☑ Ensure personnel are trained

Per the Minimum Standards, you must include all of these in your organization's insider threat program.

Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 4: Evaluating Personnel Security Information

Introduction

Objective

The Minimum Standards require your program to ensure access to relevant personnel security information in order to effectively combat the insider threat. In this lesson, you will review strategies for collecting personnel security information and see how information drawn from multiple sources can be beneficial in identifying potential insider threats.

Collecting Information

Information Sources

Ensuring that personnel security information is accessible to stakeholders in a timely manner first requires organizational components to share information. In doing this, you need to gather information from a variety of sources that includes, but is not limited to: Counterintelligence, security, human resources, and Information assurance.

Information collected from multiple sources assists your program in creating a comprehensive picture of a potential insider threat.

Counterintelligence

Information from counterintelligence includes, but may not be limited to counterintelligence files, foreign travel, and foreign contacts.

Security

Information from security should include, but may not be limited to: a variety of records and reports, security clearance adjudications, as well as information security clearance adjudications. Take a moment to review this list of possible security information sources.

- Facility access records
- Financial disclosure filings
- Security incident files
- Serious incident reports
- Inspector General reports
- Security clearance adjudications
- Polygraph results
- Foreign travel
- Foreign contacts

Human Resources

Information from human resources may include personnel files, payroll information, and other files. Take a moment to review this list of possible human resources information sources.

- Personnel files
- Payroll and voucher files
- Outside work/activities requests
- Disciplinary files

Information Assurance

Possible information from information assurance, or IA, might include different types of network access information and logs. Take a moment to review this list of possible IA information sources.

- Personnel usernames and aliases
- Levels of network access
- Unauthorized use of removable media
- Print logs
- IT audit logs

Evaluating Information

Collecting information from multiple sources will assist your program in creating a comprehensive picture of an individual. Evaluated as a whole, this picture may help confirm a potential insider threat. For example, a print log might show that an individual has been printing an unusually large amount of documents. On its own, this might not raise any flags – there could be a reasonable explanation for the printing. However, combining it with additional pieces of information might change how you see the situation.

Example

Notice the information from the employee's disciplinary file: Her performance has dropped and it's noted that she is hostile toward coworkers and managers.

from Disciplinary File

…the employee's performance has dropped off significantly…

…often hostile towards coworkers and managers…

Also note times listed in the Facility Access Records. This is outside of regular duty hours and, as it turns out, some of these times coincide with the increased print activity previously noted.

from Facility Access Records

Employee Access Time Log

Wednesday	11:34PM
Saturday	08:15PM
Sunday	04:42PM

Viewed together, this information should raise some concerns.

Review Activity

An employee was recently stopped for attempting to leave a secured area with a classified document. Although the employee claimed it was unintentional, this was the second time this had happened.

Select the files you may want to review concerning the potential insider threat.

□ IT audit logs
□ Levels of network access
□ Personnel files
□ Security incident files

Answer Key

Review Activity

An employee was recently stopped for attempting to leave a secured area with a classified document. Although the employee claimed it was unintentional, this was the second time this had happened.

Select the files you may want to review concerning the potential insider threat.

- ☑ IT audit logs
- ☑ Levels of network access
- ☑ Personnel files
- ☑ Security incident files

In order to build a comprehensive picture of the individual, you should review all of these sources of information.

Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 5: Monitoring User Activity on Classified Networks

Introduction

Objectives

The Minimum Standards require your program to include the capability to monitor user activity on classified networks. This is an essential component in combatting the insider threat.

In this lesson, you will learn about program strategies for such monitoring.

What to Monitor

Activities to Monitor

Monitoring activity on classified networks is essential for any insider threat program. Successful monitoring will involve several levels of activities.

The first aspect is governance – that is, the policies and procedures that an organization implements to protect their information systems and networks. These policies set the foundation for monitoring.

Once policies are in place, system activities, including network and computer system access, must also be considered and monitored.

Finally, an insider threat program must also monitor user activities so that user interactions on the network and information systems can be monitored.

Each level of activity is equally important and you should incorporate all of them into your insider threat program to best mitigate the risk of insider threats.

Governance

Governance, or the policies and procedures you enact for your insider threat program, will guide your efforts in monitoring user activity on your organization's networks.

These should include user and group management, use of privileged and special rights, and security and policy changes. Key components of governance include having employees sign agreements acknowledging monitoring and implementing banners informing users that their system and network activity is being monitored.

Monitoring these components ensures that users' access is limited to what is essential for their role. This allows you to then prioritize monitoring efforts.

It also allows you to identify users who are abusing their privileges.

System Activity Monitoring

Monitoring system activities will allow your program to identify possible system misuse.

Activities or events to monitor include logons and logoffs, system restarts and shutdowns, and root level access. Monitoring these activities identifies when the network is being accessed, any potential software installs, and whether someone is accessing or making changes to the root directory of a system or network.

User Activity Monitoring

Monitoring user activity helps identify users who are abusing their access and may be potential insider threats.

This includes monitoring file activities, such as downloads; print activities, such as files printed; and search activities. Monitoring these activities can identify abnormal user behaviors that may indicate a potential insider threat. While you cannot monitor every aspect of these activities, you can prioritize efforts as they relate to the systems and information that require the most protection.

How to Monitor

Monitoring Considerations

Once you determine what you are going to monitor, you must determine how you are going to monitor the activities and make sense of monitored activity.

First, there is an overarching consideration to take into account: Will your program monitor user activity in real time or will monitoring be event-triggered? Questions to ask include:

- How will data be integrated?
- How will data be analyzed?
- How will results be reported?

While some methods are preferable to others, budgets will likely be the determining factor of which methods are used.

Integration

In order to detect potential insider threats, your program needs to integrate the data it collects so it may be viewed as a whole. There are two common methods for integrating data – they are known as “push” and “pull.” Many programs use a combination of these two methods.

Using the push method, collected data is pushed to the central hub automatically. This streamlines the collection process and helps ensure the timely analysis of data. However, if too many requirements are programmed into the system, it may swamp the system with data.

With the pull method, an analyst retrieves data from several locations. This allows the analyst to request smaller and more specific queries. However, the timeliness and consistency of collection depends on the analyst’s workflow.

When determining how your program will integrate data, you will need to take into account your organization’s resources, staffing, and network setup.

Analysis

It is not enough to simply monitor and collect data. To be useful, the data must be analyzed to detect potential insider threats. Two common analysis methods are manual analysis and automatic analysis.

Manual analysis relies on analysts to review the data. It relies on the skills of the analysts involved and is often less expensive than automatic processing options, although the number of users and the amount of data being collected may require several analysts, resulting in higher costs.

Automatic analysis relies on algorithms to scan data, which streamlines the discovery of adverse information. However, this type of automatic processing is expensive to implement.

Reporting

Reporting is the culmination of the metrics and leads derived from integrating and analyzing collected data and is an essential component of any insider threat program. Reporting considerations include weighing the pros and cons of real-time versus event-triggered monitoring.

Real-time monitoring, while proactive, may become overwhelming if there are an insufficient number of analysts involved.

Event-triggered monitoring is more manageable because information is collected and reported only when a threshold is crossed. However, because event-triggered monitoring is reactive, it typically operates behind the threat, leaving open an opportunity for increased damage.

Review Activity

Which of the following best describes what your organization must do to meet the Minimum Standards in regards to classified network monitoring?

Select the correct response.

○ Develop policies and procedures for user monitoring and implementing user acknowledgements meet the Minimum Standards.

○ Running audit logs will catch any system abnormalities and is sufficient to meet the Minimum Standards.

○ Establishing a system of policies and procedures, system activity monitoring, and user activity monitoring is needed to meet the Minimum Standards.

Answer Key

Review Activity

Which of the following best describes what your organization must do to meet the Minimum Standards in regards to classified network monitoring?

Select the correct response.

○ Develop policies and procedures for user monitoring and implementing user acknowledgements meet the Minimum Standards.

○ Running audit logs will catch any system abnormalities and is sufficient to meet the Minimum Standards.

◉ Establishing a system of policies and procedures, system activity monitoring, and user activity monitoring is needed to meet the Minimum Standards.

Establishing policies and procedures, system activity monitoring, and user activity monitoring are equally important and are all needed to meet the Minimum Standards.

Student Guide

Establishing an Insider Threat Program for Your Organization

Lesson 6: Training Employees on the Insider Threat

Introduction

Objectives

Your program is required to provide insider threat training to insider threat program personnel and the cleared employees of your organization. In this lesson, you will review the requirements for training both insider threat program personnel and cleared employees in your organization.

Training

Insider Threat Program Personnel

The Minimum Standards require individuals assigned to the insider threat program to be fully trained in the following areas:

- Counterintelligence and security fundamentals
- Agency procedures for conducting insider threat response actions
- Applicable laws and regulations on gathering, integrating, retaining, safeguarding, and using records and data
- Applicable civil liberties and privacy laws, regulations, and policies
- Applicable investigative referral requirements

Cleared Employees

In addition to the training requirement for insider threat program personnel, the Minimum Standards also require your organization's cleared employees to complete insider threat awareness and reporting training. Individuals must complete training within 30 days of hire or assignment and complete annual refresher training thereafter.

As with insider threat personnel training, cleared employee training must cover certain topics that include:

- Current and potential threats in the work and personal environments
- The importance of detection and reporting to proper authorities
- Methods used by adversaries to recruit insiders and/or collect information
- Behavioral indicators and reporting procedures
- Counterintelligence and security reporting requirements

Obstacles

Despite the great emphasis training places on the importance of the threat, recognizing indicators, and reporting procedures, employees may have reservations about reporting a coworker. How, then, do you overcome this obstacle?

One successful strategy is to keep the focus on the welfare of the individuals involved. Odd or suspicious behaviors are often associated with life crises, such as work stress, financial pressure, divorce, and death. By reporting a coworker displaying odd or suspicious behaviors, that person may get help to resolve a life crisis.

Alternatively, reporting may prevent a crime that could have far reaching consequences for the employees of an organization and the citizens of the United States. If employees understand that reporting may help an individual and prevent them from taking harmful actions they might later regret, they may be more inclined to report what they observe.

Review Activity

It’s now time to put together the training for the cleared employees of your organization.

Select the topics that are required to be included in the training for cleared employees.

- □ Behavioral indicators and reporting procedures
- □ Methods used by adversaries to recruit insiders
- □ Risk management for the insider threat
- □ Current and potential threats in the work and personal environment

Answer Key

Review Activity

It’s now time to put together the training for the cleared employees of your organization.

Select the topics that are required to be included in the training for cleared employees.

- ☑ Behavioral indicators and reporting procedures
- ☑ Methods used by adversaries to recruit insiders
- □ Risk management for the insider threat
- ☑ Current and potential threats in the work and personal environment

The Minimum Standards require, among other topics, that behavioral indicators and reporting procedures, methods used by adversaries to recruit insiders, and current and potential threats in the work and personal environment be included in cleared employee training.

Student Guide

Establishing an Insider Threat Program for Your Organization

Course Conclusion

Course Conclusion

Course Summary

Insider threat programs seek to deter, detect, and mitigate the risk of insider threats. In this course, you learned about the minimum requirements and strategies needed to establish such a program for your organization.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- Lesson 1: Insider Threat Program Requirement
- Lesson 2: Setting Up an Insider Threat Program
- Lesson 3: Minimum Standards for an Insider Threat Program
- Lesson 4: Evaluating Personnel Security Information
- Lesson 5: Monitoring user Activity on Classified Networks
- Lesson 6: Training Employees on the Insider Threat

Course Objectives

Congratulations. You have completed the Establishing an Insider Threat Program for Your Organization course.

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

- Identify the policies and standards that inform the establishment of an insider threat program
- Identify key challenges to detecting the insider threat
- Identify key steps to establishing an insider threat program
- Identify the minimum standards for implementing an insider threat program
- Identify program strategies for:
    - Monitoring user activity on classified networks
    - Evaluating personnel security information
    - Training cleared employees on the insider threat

Glossary

Course: Establishing an Insider Threat Program for Your Organization

Access: The ability and opportunity to obtain knowledge of classified information.

Classified information: Information that has been determined pursuant to EO 13526, or any successor order, EO 12951, or any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. 2011), to require protection against unauthorized disclosure and that is marked to indicate its classified status when in documentary form.

Cleared Contractor (CC): A person or facility operating under the National Industrial Security Program (NISP), that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level (and all lower levels).

Cleared Defense Contractor (CDC): A subset of contractors cleared under the NISP who have contracts with the Department of Defense. Therefore, not all cleared contractors have contracts with DoD.

Cleared Employee: A person who has been granted access to classified information, other than the President and Vice President, employed by, or detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

Compromise: An unauthorized disclosure of classified information.

Contact: Any form of meeting, association, or communication in person; by radio, telephone, letter, computer; or other means, regardless of who initiated the contact for social, official, private, or other reasons.

Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, or other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. (EO 12333, as amended)

Departments and agencies: Refers to any ''Executive agency,'' as defined in 5 U.S.C. 105; any ''Military department'' as defined in 5 U.S.C. 102; any "independent establishment," as defined in 5 U.S.C. 104; and any other entity within the executive branch that comes into the possession of classified information.

Employee: For purposes of the National Insider Threat Policy, "employee" has the meaning provided in section 1.1(e) of EO 12968; specifically: a person, other than the President and Vice President, employed by, detailed or assigned to, a department or agency, including members of the Armed Forces; an expert or consultant to a department or agency; an industrial or commercial contractor, licensee, certificate holder, or grantee of a department or agency, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of a department or agency as determined by the appropriate department or agency head.

Espionage: Defined under Sections 792-799, Chapter 37, title 18, United States Code (reference: Sections 792-799, Chapter 37 of title 18, United States Code) and Article 106a, Uniform Code of Military Justice (UCMJ) (reference: Section 801-940, Chapter 47, of title 10, United States Code, Uniform Code of Military Justice). Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies during war or peace. Reference (Sections 792-799, Chapter 37 of title 18, United States Code) makes it an offense to gather, with the requisite intent or belief, national defense information, by going on, entering, flying over, or obtaining access by any means to any installation or place used by the United States for national defense. The method of gathering that information is immaterial. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense, which he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it may be punished under reference (Sections 792-799, Chapter 37 of title 18, United States Code). Anyone entrusted with or having lawful possession or control of information about national defense, who through gross negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of that trust may be punished under reference (Sections 792-799, Chapter 37 of title 18, United States Code). If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of reference (Sections 792-799, Chapter 37 of title 18, United States Code).

Insider: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.

Insider Threat: The threat that an insider will use their authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

National Security: A collective term encompassing both national defense and foreign relations of the United States.

Sabotage: An act or acts with the intent to injure or interfere with, or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises or utilities to include human or natural resources, under reference (Sections 792-799, Chapter 37 of title 18, United States Code).

Security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Subversion: An act or acts inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, of discipline, of the Military Forces of the United States.

Terrorism: The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Treason: Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason (see Section 2831 of title 18, U.S. Code, reference (Sections 792-799, Chapter 37 of title 18, United States Code).

Unauthorized Disclosure: A communication or physical transfer of classified information to an unauthorized recipient.

Unwitting: Inadvertent or accidental