Student Guide
Basic Hub Operations

CDSE Video
Screen 1 of 2

CDSE Center for Development of Security Excellence Learn. Perform. Protect.

Course Menu
Screen 2 of 2

Course Introduction, Functions of an Insider Threat Hub, Insider Threat Hub Operations, Insider Threat Hub Management Protocols, Course Conclusion, and Student Guides.

Course Introduction

Why an Insider Threat Hub?
Screen 1 of 3

Narrator: We've always contended with threats to our resources from trusted insiders.

Narrator: In the past we addressed threats predominantly from a security, law enforcement, Human Resources, or counterintelligence perspective. In other words, we responded, or reacted after we discovered a concerning event or identified a potential foreign nexus. The advent of the new insider threat policy means that we now take a more coherent and collaborative approach to how concerning events are addressed.

Narrator: Insider Threat Programs establish Hubs or teams of personnel from multiple disciplines. These teams are designed to put in place processes to examine concerning behaviors from a more coherent position with the intent of deterring, detecting, and mitigating risks associated with insiders. This proactive strategy often identifies and resolves issues before a potential insider becomes a threat to themselves or protected resources such as personnel, information, and property.

Narrator: Conducting Insider Threat Hub operations requires development of a carefully planned and managed program that takes into account more than just the minimum standards.

Narrator: Does your workforce have the awareness and training to notice and report potential indicators?

Narrator: Do you know how to manage and respond to insider threat events?

Narrator: Does your program have the proper policies and procedures in place to share information internally and refer required information to outside agencies when appropriate?

Narrator: Do you have the support of your organization's leadership?

Screen text: Select Next to continue.

Introduction
Screen 2 of 3

Screen text: Welcome to the Basic Hub Operations course

Narrator: This course provides Insider Threat Program Managers and operations personnel with an overview of Insider Threat Hub operations and incident response designed to gather, integrate, review, assess information, and respond to insider threats.

Screen text: Select Next to continue.

Course Objectives
Screen 3 of 3

Narrator: This course has three lessons. Completing them should take approximately 60 minutes. Please review the course objectives listed on the screen.

Screen text:

- Given instruction, the student will be able to explain the role and purpose of an Insider Threat program and Hub.
- Given instruction, the student will be able to explain Insider Threat Hub Operations.
- Given instruction, the student will be able to describe Insider Threat Hub management processes.

Screen text: Select Next to continue.

Lesson 1: Functions of an Insider Threat Hub

Functions of an Insider Threat Hub Lesson Objectives
Screen 1 of 8

Narrator: Before we dive into the functions of an Insider Threat Hub, please review the objectives for this lesson.

Screen text: Lesson 1 Objectives
- Describe the functions of an Insider Threat Hub.
- Explain Insider Threat Hub requirements.

Screen text: Select Next to continue.

What is Insider Threat?
Screen 2 of 8

Narrator: Let's start by defining insider threat.

Screen text: What is Insider Threat? Select each policy to view its definition of an insider threat.

Narrator: While the exact definition depends on the policy under which your organization operates, generally, an insider threat is someone with authorized access who uses that access, wittingly or unwittingly, to either harm or degrade organizational resources. This can include, but is not limited to, the loss, compromise, or unauthorized disclosure of protected information (classified or unclassified); kinetic threats to include violent events against self or others; and threats to Government installations, facilities, personnel, missions, or resources.

Executive Order 13587 Popup:
Screen text: "Insider Threat means the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of 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."

DoDD 5205.16 Popup:
Screen text**:** "Insider Threat. The threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. 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 Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M Popup:
Screen text**:** "Insider Threat. 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."

Screen text: Select Next to continue.

What is the Insider Threat Hub?
Screen 3 of 8

Narrator: The National Insider Threat Policy requires that DoD components and Federal Agencies accessing classified information develop "…effective Insider Threat programs within departments and agencies to deter, detect, and mitigate actions by employees who may represent a threat to national security."

Screen text: What is the Insider Threat Hub? An Insider Threat Hub is a multi-disciplinary staff element or activity established by an organization that possesses an integrated capability to monitor, audit, fuse, and analyze incoming information for insider threat detection and mitigation. Hub personnel will be able to analyze information and activity indicative of an insider risk and refer that data to the appropriate officials for investigation and/or resolution.

Narrator: Part of this requirement is the establishment of a team or Hub. "Best practices dictate that the Hub" include Legal Counsel, Law enforcement, Security, Counterintelligence, Cybersecurity, Mental health and behavioral science, and Human Resources or Human Capital disciplines to effectively counter insider threats to our national security.

Narrator: Industry requirements, as identified under NISPOM Change 2, require facilities to establish an Insider Threat program group consisting of program personnel from offices across the contractor's facility, based on the organization's size and operation.

Narrator: The size and complexity of your organization will determine the exact makeup of your Insider Threat team or Hub. Regardless, all actions undertaken by the Insider Threat Hub must respect the privacy and civil liberties of the workforce.

Screen text: Select Next to continue.

What is the Purpose of an Insider Threat Hub?
Screen 4 of 8

Narrator: Insider Threat Hubs take proactive measures to deter, detect, mitigate, and report the threats associated with trusted insiders. The Hub identifies anomalous behaviors that may indicate an individual poses a risk. Early identification allows Insider Threat program personnel to focus on an individual's issues of concern or stressors and deploy appropriate mitigation responses. When necessary, the team shares relevant information from each discipline with organizational leadership to facilitate timely, informed decision-making and reports information outside the organization as required by policy or regulation.

Screen text: What is the Purpose of an Insider Threat Hub? An Insider Threat program is intended to be a proactive approach to deter, detect, mitigate, and report the threat associated with trusted insiders. Hub team members from each discipline work together to monitor, analyze, report, and respond to behaviors that could be considered indicative of an insider threat.

Deter Popup:

Narrator: Insider Threat Hubs deter potential insider threats by instituting appropriate security countermeasures, including awareness programs.

Screen text: Deter: Insider Threat Hubs deter potential insider threats by instituting appropriate security countermeasures, including awareness programs.

Detect Popup:

Narrator: Insider Threat Hubs detect individuals at risk of becoming insider threats by identifying potential risk indicators. These observable and reportable behaviors or activities may indicate an individual is at greater risk of becoming a threat.

Screen text: Detect: Insider Threat Hubs detect individuals at risk of becoming insider threats by identifying potential risk indicators. These observable and reportable behaviors or activities may indicate an individual is at greater risk of becoming a threat.

Mitigate Popup:

Narrator: Insider Threat Hubs mitigate the risks potential insider threats pose. One of the goals of the Insider Threat Hub is to identify and mitigate issues before they escalate, but sometimes programs become involved in the middle of an incident or event or even after the fact.

Screen text: Mitigate: Insider Threat Hubs mitigate the risks potential insider threats pose. One of the goals of the Insider Threat Hub is to identify and mitigate issues before they escalate, but sometimes programs become involved in the middle of an incident or event or even after the fact.

Report Popup:

Narrator: Insider Threat Hubs are required to report information about actual or potential insider threats and can refer insider threat data to the appropriate officials to investigate or otherwise resolve.

Screen text: Report: Insider Threat Hubs are required to report information about actual or potential insider threats and can refer insider threat data to the appropriate officials to investigate or otherwise resolve.

Screen text: Select Next to continue.

What are the Insider Threat Hub Requirements?
Screen 5 of 8

Narrator: Requirements for the Insider Threat program articulate minimum standards for establishing a program. The National Insider Threat Policy and Minimum Standards lay the foundation for your program. It outlines the policy and general responsibilities. DoD Directive 5205.16 establishes policy and assigns responsibilities within DoD to develop and maintain an Insider Threat program. DoD Instruction 5205.83 established the DoD Insider Threat Management and Analysis Center, also known as the "DITMAC," and requires DoD Hubs to timely report insider threat matters meeting certain thresholds to the DITMAC. National Industrial Security Program Operating Manual, or NISPOM, prescribes the requirements for Industry Insider Threat programs.

Screen text: What are the Insider Threat Hub Requirements?

- Executive Order 13587
- Presidential Memorandum -- National Insider Threat Policy and Minimum Standards (Nov 21, 2012)
- DoDD 5205.16, The DoD Insider Threat Program
- DoDI 5205.83 DoD Insider Threat Management and Analysis Center
- National Industrial Security Program Operating Manual (NISPOM) change 2
  - Industry Insider Threat Program Job Aid (Interprets NISPOM change 2)

Narrator: Keep in mind that these are the minimum standards. To be truly effective, Insider Threat Hubs must continually evaluate their program, employ best practices, and look for opportunities to enhance their program as they develop and review policies and procedures.

Narrator: You can view these requirements on the CDSE Insider Threat Toolkit Policy/Legal page.

Screen text: Select Next to continue.

Knowledge Check 1
Screen 6 of 8

Screen text: What process is your Insider Threat Hub performing if they are attempting to prevent insiders' personal issues from escalating into threats? Select the best response.

- Deter
- Detect
- Mitigate
- Report

Screen text: Select Next to continue.

Knowledge Check 2
Screen 7 of 8

Screen text: Which Insider Threat Program policy would apply to an U.S. Air Force component with military, civilian, and contractor personnel? Select the best response.

- DoDD 5205.16
- DoDI 5240.26
- NISPOM Change 2
- DoDD 5240.16

Screen text: Select Next to continue.

Lesson Summary
Screen 8 of 8

Narrator: In this lesson, we described the functions of an Insider Threat Hub and explained its requirements. Knowing the functions and requirements of an Insider Threat Hub gives you a solid foundation to build on your knowledge of basic Hub operations. Select Next to view another lesson.

Screen text: Select Next to view another lesson.

Lesson 2: Insider Threat Hub Operations

Insider Threat Hub Operations Lesson Objectives
Screen 1 of 9

Narrator: Now that we understand the functions and requirements of an Insider Threat Hub, let's discuss the basic operations that your program will perform. Please review the objectives for this lesson.

Screen text: Lesson Objectives
- List the requirements for establishing an Insider Threat Hub.
- Describe the implementation of insider threat operations.

Screen text: Select next to continue.

Requirements for Establishing a Hub
Screen 2 of 9

Narrator: If your organization is new to the Insider Threat program, establishing an Insider Threat Hub will be one of the first actions taken. The responsibility for establishing a Hub belongs to the Insider Threat Senior Official and/or Program Manager. However, the entire team will be involved as the program's policy and procedures are developed.

Narrator: The first item on the list is to identify the program office. What really needs to be determined is how the team will be structured and where it will be located? Does your organization have the ability to house the team in a single location? Or, are the team members geographically separated and must rely on virtual communications to conduct operations? This of course is dependent on how the organization is structured and what works best for the team.

Screen text: Establishing an Insider Threat Hub "To Do" List
1. Identify Program Office

Narrator: Staffing and resources is the next item on your list. An organization selects the Insider Threat program Senior Leader or official. In some cases, this person may also serve as the Hub Program Manager that oversees day-to-day operations. They will work with the organization's senior leadership to determine resource and staffing needs.

Narrator: Once established, it is the Hub Program Manager's responsibility to train, exercise, and equip the Hub team with the knowledge, skills, abilities, and resources to conduct counter-insider threat duties. The National Policy and Minimum Standards identify the minimum training requirements for federal Insider Threat program personnel. NISPOM Change 2 identifies these requirements for industry programs.

Screen text: Establishing an Insider Threat Hub "To Do" List
1. Identify Program Office
2. Staffing and Resources

Narrator: The next item on the list is to establish organization rules for how the Hub operates within the organization, and how it coordinates its activities within the organization. These rules and policies will be specific to your organization. National, DoD, and industry policies and guidance can only go so far. Every agency or organization will have functions and activities that are specific to them. It is up to the Hub team to develop policy and procedures that meet the minimum standards and are detailed enough to be effective for their organization.

Screen text: Establishing up an Insider Threat Hub "To Do" List
1. Identify Program Office
2. Staffing and Resources
3. Establish Organization Rules and Policy

Narrator: As part of rule and policy development, the Hub team must also identify consequences for violations of internal rules committed by Hub team members. Insider Threat team members must maintain standards of professional conduct like any other personnel. However, because you're dealing with extremely sensitive information it's important that you clarify these responsibilities up front.

Screen text: Establishing an Insider Threat Hub "To Do" List
1. Identify Program Office
2. Staffing and Resources
3. Establish Organization Rules and Policy
4. Institute Consequences for Established Rule/Policy Violations

Narrator: As a best practice, you may want to establish a continuity of operations plan. This plan will lay out your team's strategies for continuing the program's operations in the event of disruptions related to natural disasters, terror attacks, cyber-attacks, or equipment failures. FEMA has developed a useful template for these types of plans. When your team is ready to start building this plan, you can start with the template or develop your own.

Screen text: Establishing an Insider Threat Hub "To Do" List
1. Identify Program Office
2. Staffing and Resources
3. Establish Organization Rules and Policy
4. Institute Consequences for Established Rule /Policy Violations
5. Continuity of Operations Planning (See FEMA COOP plan)

Narrator: Once the training is complete, policies are in place, and plans are established, the team needs to ensure that all Insider Threat Program personnel are trained to deter, detect, mitigate, and respond to insider threats. Insider Threat Program personnel must be able to appropriately respond to incident reporting, protect privacy and civil liberties, support mitigation options, and refer matters as required.

Screen text: Establishing an Insider Threat Hub "To Do" List
1. Identify Program Office
2. Staffing and Resources

3. Establish Organization Rules and Policy
4. Institute Consequences for Established Rule /Policy Violations
5. Continuity of Operations Planning (See FEMA COOP plan)
6. Communicate Program Requirements to Staff and Contractors

Narrator: Once the staff is aware of the requirements, you must ensure policies and procedures are being followed by conducting self-assessments. Self-assessments help you determine whether your program is meeting requirements and operating effectively. This information can guide performance measures that lead to more efficient and effective programs.

Screen text: Establishing an Insider Threat Hub "To Do" List
1. Identify Program Office
2. Staffing and Resources
3. Establish Organization Rules and Policy
4. Institute Consequences for Established Rule /Policy Violations
5. Continuity of Operations Planning (See FEMA COOP plan)
6. Communicate Program Requirements to Staff and Contractors
7. Conduct Internal Spot Checks

Narrator: Follow this list to guide you through the process of establishing your Insider Threat Hub.

Screen text: Select next to continue.

Implementing Insider Threat Operations – Deter
Screen 3 of 9

Narrator: The purpose of the Insider threat program is to proactively deter, detect, mitigate, and report threats associated with trusted insiders. These actions make up the daily operations of your Insider Threat Hub. Let's look at each of these individually. How does your program deter?

Screen text: Implementing Insider Threat Operations
- Deter
- Detect
- Mitigate
- Report

Screen text: Implementing Insider Threat Operations Deter
Select each tab to learn more.

Narrator: Deterrence efforts are designed to prevent insider threats from manifesting in the first place. Deterrence programs are more than just general awareness. They should take into account multiple facets of your organization and Hub activities.

Integrate Personnel Security tab:

Narrator: Integrating personnel security is a great first step in deterring insider threats. Building a good working relationship with the personnel security team is vital. They can help the Hub team understand pre-employment vetting activities and define their role in mitigating risk prior to human capital or human resources on-boarding personnel.

Screen text: Integrate Personnel Security
- Build a relationship with the Personnel Security Team
- Review Pre-employment vetting activities

Train/Exercise the Workforce tab:

Narrator: You must train and exercise the organization's workforce. Covered employees must complete initial and annual Insider Threat Awareness training. You may also responsible for maintaining workforce awareness of insider threats and employee reporting responsibilities. As an aid, CDSE has instituted a year-round vigilance campaign. Lastly, you will conduct internal evaluations. These are small exercises used to test your workforce's knowledge of insider threat indicators and reporting requirements. These exercises do not have to be elaborate but should help you gauge the effectiveness of your program. You may use information from these evaluations to adjust your training and awareness program to ensure effectiveness.

Screen text: Train and exercise the workforce
- Provide mandatory training
- Maintain workforce awareness and disseminate insider threat vigilance materials
- Internal Evaluation

Develop "Normal Activity" Baseline tab:

Narrator: Having a day-to-day operating baseline will make deviations or anomalies stand out from normal activities. It will also help determine what your user activity monitoring triggers should be.

Screen text: Develop "Normal Activity" Baseline
- Use to establish the organization's normal day-to-day operations

Institute Internal and Security Controls tab:

Narrator: Once a "Normal Activity" baseline is established, internal and security controls help us identify deviations from the baseline. For example, user activity monitoring could help identify a rash of IT system misuses that may suggest an employee needs some re-training. Another example would be access control logs indicating an employee is working irregular hours or has unexplained absences from work. You would want to look into this further. Internal and security controls can help identify important risk factors.

Screen text: Institute Internal and Security Controls
- Establish and monitor controls for potential risk indicators

Encourage Reporting tab:

Narrator: Individuals should be encouraged to report on issues they may have or the actions of others. One of the goals of an Insider Threat Hub is to deter adverse actions by pointing those asking for assistance to resources that can help them. The challenge is to have people see the Insider Threat program as a resource rather than a punitive element. You can build this rapport by informing the workforce of your program, the mission, and its goals; by respecting privacy and civil liberties, and by deploying appropriate insider threat mitigation responses.

Your program must establish reporting procedures for the general workforce. Those that witness potential indicators should know exactly, when, where, and how they can report the information. Prepare procedures for "walk-ins" or those that may want to report their information face to face. Procedures should also include hotlines or dedicated email addresses.

Finally, your Hub must consider the concept of organizational justice. Organizational justice refers to employee perceptions of fairness in the workplace. Labor relations can have an overall effect on the number of insider threat incidents you see. The worse the labor relations are, the more incidents you may encounter. Counterproductive workplace environments have consequences that can lead to disgruntlement. Organizational leadership that develops a positive workplace environment keeps the workforce engaged and productive.

This same concept applies to the Insider Threat program. Ensuring appropriate mitigation response options and the protection of privacy and civil liberties in the conduct of your duties will minimize negative outcomes from maladaptive responses. Being responsive to workforce concerns is a great way to build rapport with personnel; encourage future reporting; and ultimately mitigate risk.

Screen text: Encourage Reporting (including self-reporting)
- Workforce should see the Insider Threat Program as a resource
- Establish procedures for walk-in reporting
- Federal Programs will institute Electronic reporting methods per the National Minimum Standards “Establish and promote an internal network site accessible to all cleared employees to provide insider threat reference material, including indicators of insider threat behavior, applicable reporting requirements and procedures, and provide a secure electronic means of reporting matters to the Insider Threat program”
- Industry programs should consider electronic reporting methods
- All organizations should consider Organizational Justice concepts

Screen text: Select next to continue.

Implementing Insider Threat Operations – Detect
Screen 4 of 9

Narrator: Another essential daily Insider Threat Hub Operation activity is insider threat detection.

Screen text: Implementing Insider Threat Operations - Detect. Select each tab to learn more.

Ensure cross-function coordination tab:

Narrator: Cross function coordination is the key to effective detection. You must determine who will lead the team; how the team will communicate; and how the team will integrate contributors who are not part of the organization's Insider Threat program. The team must decide the role that each of these external partners will play. For example, they may serve as a reviewer of the team's work, or a consultant that is used on an as-needed basis.

Screen text: Ensure Cross-function Coordination
- From a practical standpoint, how will the team communicate?
- Who will lead the team?
- How will the team integrate contributors who are not part of the organization's Insider Threat program? External contributors may include:
  - Individuals from team member's professional networks
  - Other components, agencies, or companies such as The National Insider Threat Task Force and, for DoD Components
  - The DoD Insider Threat Management and Analysis Center or DITMAC

Monitor Activity tab:

Narrator: User Activity Monitoring is the technical capability to observe and record the actions and activities of an individual operating on your computer networks, in order to detect potential risk indicators and to support mitigation responses. For additional information on developing UAM, find Insider Threat Indicators in User Activity Monitoring Job Aid in the course resources.

Screen text: Monitor Activity
- User Activity Monitoring (UAM)
- Tools and Reports that Assist Data Collection / UAM Trigger / Information Security Policies

Perform Risk-based Analytics tab:

Narrator: Risk based analytics allow Insider Threat Hubs to manage risk in complex threat environments. The process of identifying assets, assessing threats and vulnerabilities, evaluating risk, and identifying countermeasures can help determine the risks most closely associated with trusted insiders and the best methods to deter and mitigate them. It also allows your organization to differentiate between exigent threats to your enterprise and less pressing matters.

Review the Risk Management for DoD Security Programs Student Guide for more information.

Screen text: Perform Risk-based Analytics
- Meeting today's security challenges
- Risk management five-step process
  - Assess assets
  - Assess threats
  - Assess vulnerabilities
  - Assess risks
  - Determine countermeasures

Gather, Integrate, Review, Assess, and Response Indicators tab:

Narrator: Your Hub will need to gather, integrate, review, assess, and respond to threat indicators. To do that, you need to establish data collection protocols. Indicators provide a gauge to measure the state of a situation. To be effective, indicators must meet several criteria. First, they should be observable, from a reliable source, and be gathered in accordance with laws and regulations. Next, indicators should be valid, reliable, relevant, and considered in context. Insider Threat programs must use consistent data collection methods, or the data will be unreliable. All data collection protocols must be developed in coordination with legal guidance and any applicable systems of records notice. Prohibited actions must be clearly identified to ensure that you protect the privacy and civil liberties of the workforce in the conduct of your duties. This clarity can also prevent Insider Threat team members from inadvertently overstepping their bounds.

Screen text: Gather, Integrate, Review, Assess, and Response Indicators
- Establish data collection protocols
- Engage in responsible information sharing
- Prohibited Actions

Create Auditable Records of Actions Taken tab:

Narrator: So why would you want to create auditable records of actions? Well, the actions performed by your program may come under scrutiny and having a clear record of program actions may protect you and your organization from legal repercussions and help external agencies when you refer incidents. They also help ensure you follow the established guidelines and identify criteria that need to be adjusted. For instance, you may review a memorandum of action and discover one of your threat indicator triggers are not set properly and needs to be adjusted. Please check out the memorandum of action template. It may be helpful when developing your record keeping methods.

Screen text: Create Auditable Records of Actions Taken
- MOA Template

Share Information as Appropriate tab:

Narrator: Responsible information sharing is critical to the success of your program. Developing protocols – such as when to report or refer matters, approved methods for information transmittal, and the identification of authorized recipients – is an essential function of the program and one that will require close coordination with your legal team. No matter how your Hub decides to do this, you must ensure that you consider the privacy and civil liberties of your employees as part of your processes and practices.

Screen text: Share Information as Appropriate
- Adhere to protocols established for your program
- Protect privacy and civil liberties when sharing

Screen text: Select next to continue.

Implementing Insider Threat Operations – Mitigate
Screen 5 of 9

Narrator: To be effective, Insider Threat programs must be on the lookout for potential issues before they pose a threat, have a risk assessment process in place, address identified issues adequately, and take actions that minimize risk while avoiding those that escalate risk. In most cases, proactive mitigation responses provide positive outcomes for both the organization and the individual. This allows you to protect information, facilities, and personnel, retain valuable employees, and offers intervention to help alleviate the individual's stressors.

Screen text: Implementing Insider Threat Operations
Mitigate
Select each tab to learn more.

Conduct Hub Team Case Review tab:

Narrator: Developing a case review process will help your Hub review incidents and conduct analysis on insider threat matters. The case review process includes receiving the report, reviewing and gathering additional information, assessing the situation, and responding to the situation.

Screen text: Conduct Hub Team Case Review
- Develop and Implement a Case Review Process
  - Receive Report
  - Review and gather additional information
  - Assess the situation
  - Respond to the situation

Determine and Implement Appropriate Response tab:

Narrator: Your Hub's responses are situationally dependent, but may include recommendations such as suspending access to information; taking personnel actions such as counseling, referral, or termination; organizational responses that may require changes to policy or procedures; and finally, responses could require increased or additional training.

Screen text: Determine and Implement Appropriate Response
Examples include:
- Suspended access
- Personnel action
- Organizational response
- Increased training

Produce an Insider Threat Incident Outcome Report tab:

Narrator: Your Hub should create a record of the incident outcome. There is no standard form for this, so you could incorporate this information in your Records of Actions form or create a new format. You may also create or coordinate with other elements to develop a "Damage Assessment" or "After Acton Report" that explains the damage to national security, personnel, facilities, or other resources. The Hub will need to work with the legal team and any other contributing elements to ensure the report is stored and retained appropriately.

Screen text: Produce an Insider Threat Incident Outcome Report
- Create a record of the incident outcome
- After Action Report
- Damage Assessment

Execute Insider Threat Incident Report Referral Actions tab:

Narrator: Once your report is complete or sometimes while you are working on it, you may need to execute referral actions. The Insider Threat Hub may refer the matter internally to its agency's security office, cybersecurity, or human resources for action to mitigate risks. It may also be referred elsewhere in the agency, if appropriate.
Human Resource and mental health team members can assist with counseling referrals or prescribed human resource interventions which may be corrective in nature. They deal with Employee Assistance Programs for resources in financial counseling, lending programs, mental health, and other well-being programs. Hub members from the various security disciplines, whether cyber, personnel, information, or physical, can assist with mitigation response options such as updating security protocols, adjusting UAM or other inspections, and providing basic security training and awareness to the workforce.

Some insider threat incidents may warrant external referrals to counterintelligence or law enforcement authorities. For DoD component insider threats, this includes referral of certain threshold level events to the DoD Insider Threat Management and Analysis Center or DITMAC. Not all incidents will meet reporting thresholds or result in an arrest. However, you must still

work with the referral agency and your organizations legal counsel to ensure that any information gathered during the incident is handled properly in case it is determined to be evidence in subsequent actions such as inquiries or investigations.

Screen text: Execute Insider Threat Incident Report Referral Actions
Internal referrals

- Counterintelligence or law enforcement referrals
- DITMAC (for DoD)
- Referral to counseling

Screen text: Select next to continue.

Knowledge Check 1
Screen 6 of 9

Screen text: If your team is developing a strategy for disruptions caused by natural disasters, terror attacks, cyber-attacks, or equipment failures, which plan would they be working on? Select the best response.

- Continuity of Operations Plan
- Organization Policy Plan
- Staff and Contractors Requirements Plan
- Internal Spot Checks Plan

Screen text: Select next to continue.

Knowledge Check 2
Screen 7 of 9

Screen text: An organization was implementing their insider threat operations and was developing a "normal activity" baseline as part of its deterrence operations. Why is establishing a "normal activity" baseline important? Select the best response.

- It will make deviations or anomalies stand out from normal activities.
- It will help determine the Hub's staffing requirements.
- It will identify the potential insider threats within the organization
- It will be a key indicator of the workforce's current level of training.

Screen text: Select next to continue.

Knowledge Check 3
Screen 8 of 9

Screen text: If you are developing a report that documents the results of a particular insider threat event, which insider threat report would you be writing? Select the best response.

- Incident Outcome Report
- Intelligence Report

- Organizational Justice Report
- Referral Actions Report

Screen text: Select next to continue.

Lesson Summary
Screen 9 of 9

Narrator: In this lesson, we discussed the requirements involved in establishing an Insider Threat Hub and described its day-to-day operational activities. Select Next to view another lesson.

Screen text: Select Next to view another lesson.

Lesson 3: Insider Threat Hub Management Protocols

Insider Threat Hub Management Protocols Lesson Objectives
Screen 1 of 12

Narrator: You may have seen organizations where the staff understands their procedures and daily operations seem to function smoothly. This level of efficiency did not happen by accident. More likely, the leadership took the time to craft detailed procedures that guide the staff's and management's actions and expectations. This lesson will focus on the procedures or management protocols, you will need to develop to ensure your Insider Threat Hub is ready to handle situations when they arise. Please review the objectives for this lesson.

Screen text: Lesson Objectives
- Explain how to track and implement new/revised insider threat policy.
- Describe best practices for establishing Insider Threat Program Standard Operating Procedures.
- Explain how to integrate the Insider Threat program into larger organizational missions and national security.
- Explain how to establish an Insider Threat program evaluation plan.

Screen text: Select next to continue.

Management Protocols
Screen 2 of 12

Narrator: What protocols should you have in place to ensure your Insider threat Hub can respond quickly and consistently? It would be nearly impossible to write a protocol for every situation that you could encounter as a Hub member. However, you should standardize some procedures to ensure the members of the Insider Threat team are not reinventing the wheel each time those situations arise. Some of the basic protocols to consider developing for your Hub include procedures for tracking and implementing policy; formal and informal agreements; integrating the program into the organizational mission; and a program evaluation plan. These topics are addressed in more detail in the CDSE course: Preserving Investigative and Operational Viability. Let's take a deeper look at each of these protocols.

Screen text: Management Protocols
- Tracking and Implementing Policy
- Formal and Informal Agreements
- Integrating the program into the Organizational Mission
- Program Evaluation Plan

Screen text: Select next to continue.

Tracking and Implementing Policy
Screen 3 of 12

Narrator: All Insider Threat Hubs should have something in writing designating responsibility for keeping up to date with policy changes. Follow policy releases, updates, and modifications to incorporate new requirements and ensure you are always acting under proper legal authority.

Screen text: Management Protocols
- Tracking and Implementing Insider Threat Policy

Narrator: To stay up to date, many policy issuers offer email service that notifies you when they post policy updates. Alternatively, regularly check their websites for updates. See the Defense Security Service for industry programs, the Defense Technical Information Center for DoD programs, and the National Insider Threat Task Force for Federal Programs.

Screen text: Management Protocols
- Tracking and Implementing Insider Threat Policy
- Stay up to date with the policy issuers

Narrator: However, policy issuers' sites are not the only places you can stay up to date with policy changes. The CDSE's Insider Threat Toolkit also lists the latest policies for you. Other resources for tracking policy issuances are your colleagues and working groups. You may learn about upcoming policy changes by staying connected to the larger community and attending Insider Threat working groups or forums.

Screen text: Management Protocols
- Tracking and Implementing Insider Threat Policy
- Stay up to date with the policy issuers
- CDSE Insider Threat Toolkit, working groups, and forums

Narrator: Anytime you receive new policy information, you need to run it past your Hub's legal team. The legal team must be aware of any changes to policy, so they can assess possible implications for your program.

Screen text: Management Protocols
- Tracking and Implementing Insider Threat Policy
    - Stay up to date with the policy issuers
    - CDSE Insider Threat Toolkit, working groups, and forums
    - Engage your legal team when new releases are issued

Screen text: Select next to continue.

Formal and Informal Agreements Information
Screen 4 of 12

Narrator: Developing protocols for formal and informal agreements is critical to the success of your Insider Threat program. These agreements lay the groundwork for conducting business with internal and external organizational elements your Hub will need to work with. They include Law Enforcement or LE and Counterintelligence or CI. Coordinate with your legal team when developing relationships with these outside agencies. Some laws, policies, and directives require an Insider Threat Hub to refer certain insider threat matters to external CI and/or LE entities. Your legal team's expertise and assistance will be necessary to develop your policy, procedures, and agreements. Select the image to view these matters.

Narrator: Industry programs under the NISPOM may be required to inform their senior leadership and/or consult with DSS for guidance on any further actions. Planning this coordination in advance can make for a more effective incident response and mitigation. Ensure that you have a communication method for your internal leadership as well as your DSS Industrial Security Representative and/or CI Special Agent.
It's important to remember that most incidents handled by your program will not result in the apprehension of a spy or even identify someone committing a crime. The main goal of the program is to detect potential risk indicators, determine whether a threat exists, and if so mitigate it appropriately.

Screen Text: Management Protocols
- Formal and Informal Agreements

Popup Screen text:
Insider threat matters that require referral to LE and/or CI:
- Threats and acts of violence
- Loss or compromise of classified information
- Physical or cyber breaches
- Foreign intelligence entity activity
- Criminal activity

Screen text: Select next to continue.

Developing Standard Operating Procedures
Screen 5 of 12

Narrator: Now let's discuss how to develop your Hub's standard operating procedures or SOPs. Insider Threat Hubs can handle most matters internally but, as you know, some incidents require reporting and referral actions that may result in law enforcement or counterintelligence investigations, inquiries, operations, and/or legal proceedings. Your actions can affect the outcome of cases. Develop your internal policies, procedures, and authorities in a way that ensures your activities do not produce negative impacts on cases. All Insider Threat Hub team members should understand how to preserve investigative and operational viability. More information can be found in CDSE INT220, Preserving Investigative and Operational Viability.

Screen text: Management Protocols

- Developing Standard Operating Procedures

Four selectable buttons appear on screen labeled:
Communications Plan
Non-Alerting Protocols
Reporting and Referral Timelines
Handling and Seizure of Information of Potential Evidentiary Value

Screen text: Select each procedure to learn more.

Communications Plan Popup:

Narrator: One best practice is to develop a communications plan. A good plan describes the protocol for discussing insider threat matters with the media and other external elements. Your Insider Threat Program Manager will work with the public affairs office and legal counsel to develop your communications plan and establish guidelines for what information is releasable to the public and by whom. Follow the guidance provided by the communications plan and your public affairs office. The things you say may have far-reaching impacts on potential operations or investigations, individuals, and ultimately the effectiveness of Insider Threat Hub Operations.

Screen text: Communications Plan Example: Any public statements regarding insider threat matters should be made exclusively by your organizations public affairs or public relations office and in coordination with legal guidance.

Non-Alerting Protocols Popup:

Narrator: Take steps to avoid alerting subjects of a potential inquiry, investigation, or operation whenever your program conducts its internal situational assessment. Insider Threat Hub protocols should determine how and when you limit or prohibit interviews of subjects or checks of certain data sets that have alert capabilities. Also, consider incorporating non-alerting protocols that may limit the Hub's internal distribution of information. A non-alerting protocol limits the number of program personnel who have knowledge of the most sensitive matters.

Screen text: Non-Alerting Protocols Example: Insider Threat Hub actions, including certain records checks and interviews with co-workers and supervisors, may inadvertently alert potential subjects of investigation or inquiry. Implement protocols to minimize the potential of alert associated with insider threat program activities.

Reporting and Referral Timelines Popup:

Narrator: Delayed reporting or failure to make timely referrals may increase your organization's insider threat risk. You can mitigate that risk by incorporating timelines for reporting and referrals in SOPs. Delayed reporting or referral may negatively impact investigations, inquiries, or operations carried out by CI or LE. Significant time lapses between suspected activities may

impede the ability to successfully investigate or prosecute wrongdoing. That's why it's important to work with your General Counsel to determine the best course of action during each referral process.

Screen text: Reporting and Referral Timelines Example:
The Defense Insider Threat Management Analysis Center (DITMAC) sets reporting thresholds for DoD Insider Threat programs to ensure that DITMAC can integrate data from multiple sources and keep the risk low to both the component and the DoD. Delayed reporting impacts the ability of all organizations to appropriately mitigate risk.

Handling and Seizure of Information of Potential Evidentiary Value Popup:

Narrator: While Insider Threat Hubs do not conduct investigations, your program's standard operating procedures should include provisions for proper handling and documentation of any items seized in the course of your actions that may have evidentiary value. Your Hub's legal team can tell you, there are many legal rules to follow when seizing, handling, and storing information. When developing procedures involving information with potential evidentiary value, it's a best practice to coordinate with the Inspector General and/or your General Counsel.

Screen text: Handling and Seizure of Information of Potential Evidentiary Value Example:
There may be rare instances when the Program must take possession of and/or transmit physical or digital information of potential evidentiary value associated with a potential insider threat.

Screen text: Select next to continue.

Knowing Your Organization
Screen 6 of 12

Narrator: Insider Threat Hub operations require integration within your organization to succeed. The Program Manager must work with the organizational leadership to ensure the program has top-down support. However, the entire team needs to advocate for the program. Highlighting the Insider Threat Hub's role in mission assurance and risk management can engender support needed from the entire organization. This requires Insider Threat Hub team members to adopt a cohesive message. Help team members deliver the same message by putting together talking points that explain the program's role.

Narrator: Participate in internal working groups and meetings to understand changes in the organization that may affect your ability to deter, detect, and or mitigate a threat. Also make sure to keep up with the larger issues affecting insider threat policy, programs, and best practices by attending community or national level workshops.

Screen text: Integrating an Insider Threat program into your organization
- Get top-down from leadership
- Advocate for the program to get support from the entire organization
- Develop talking point for team members
- Best Practices and Attend Workshops

Organization activities that may increase the risk of an insider threat incident include:

- Hiring waves
- Layoffs
- Pay freezes
- Deployments
- New computer software/systems
- New security protocols
- Program funding issues

Screen text: Select next to continue.

Evaluation Plan – Internal Audits
Screen 7 of 12

Narrator: Though they vary slightly, all insider threat policies require that you perform self-assessments of compliance with insider threat policies and standards. To meet that requirement, you need to develop an Insider Threat Program Evaluation Plan. A good program evaluation plan helps your program focus on meeting the requirements applicable to your organization and promotes continuous improvement. Do this by evaluating the program's plan, policies, procedures, and metrics. Metrics can document everything from the number of general workforce personnel training on insider threat awareness, the number of reports or indicators received, the number of incidents handled or mitigated, or the number of external referrals. These metrics help you both evaluate the effectiveness of Hub operations and advocate for resources to ensure the success of your program.

Screen text: Insider Threat Program Evaluation Plan - Internal Audits Policy
Select each policy to view its internal audits requirements.

National Insider Threat Policy Popup:

Screen text: National Insider Threat Policy
National Insider Threat Policy, General Responsibilities of Departments and Agencies:
7) Perform self-assessment of compliance with insider threat policies and standards; the results of which shall be reported to the Senior Information Sharing and Safeguarding Steering Committee.

DoDD 5205.16 Popup:

Screen text: DoDD 5205.16, ENCLOSURE 2
For DoD components and federal agencies, program self-assessments must be completed in accordance with National Minimum Standards and other appropriate policy and memoranda. DoD components can work with the DoD Insider Threat Enterprise Program Management Office for specific guidance. Federal programs should contact the National Insider Threat Task Force for additional information.

National Industry Security Program Operating Manual (NISPOM) Popup:

1-207 b. Contractor Reviews. Contractors will review their security system on a continuing basis and shall also conduct a formal self-inspection at intervals consistent with risk management principles. Self-inspections will include the following elements:

- The contractor will prepare a formal report describing the self-inspection, its findings, and resolution of issues found. The contractor will retain the formal report for DSS review through the DSS security vulnerability assessments.
- A senior management official at the cleared facility will certify to the CSA, in writing on an annual basis that a self-inspection has been conducted, senior management has been briefed on the results, appropriate corrective action has been taken, and management fully supports the security program at the cleared facility. A copy of the formal report will be forwarded to DSS.
- Self-inspections by contractors will include the review of representative samples of the contractor's derivative classification actions, as applicable.
- These self-inspections will be related to the activity, information, information systems (ISs), and conditions of the overall security program, to include an Insider Threat program; have sufficient scope, depth, and frequency; and management support in execution and remedy.

Refer to pages 61-67 of the NISP Self-Inspection Handbook

Screen text: Select next to continue.

Evaluation Plan – External Audits and Auditable Records
Screen 8 of 12

Narrator: Self-inspections help you identify and correct program issues. Staying current is important because processes, policy, and guidance are subject to change. In addition, the government retains some level of oversight to ensure Insider Threat programs keep up with the latest insider threat requirements. External audits verify that your program maintains its effectiveness. It is in your best interest to cooperate with and facilitate these audits to ensure that your program meets all the requirements and acquires assistance in areas where the program is lacking.

Screen text: Management Protocols
Insider Threat Program Evaluation Plan

- External Audits
- Depending on the organization, the program may be evaluated by:
  - DSS for Industry
  - DoD Elements and/or NITTF for DoD
  - NITTF for Federal

Narrator: One of the best ways to prepare for external audits is to create and maintain auditable records of your actions. Work with your legal team to ensure that these items are created, stored, and retained in accordance with privacy and civil liberties regulations. As you can see, keeping

good program records have several other benefits for your program as well. They become a consolidated repository of data used to measure the effectiveness of your program.

Screen text: Management Protocols
Insider Threat Program Evaluation Plan
Auditable Records of Actions

This information can be used to:

- Demonstrate compliance with Insider Threat Policy
- Develop Metrics
- Gain top-down support from your organization
- Help with risk management by identifying areas at risk
- Help justify funding for your program

Narrator: No specific format has been identified for program evaluation. Depending on your organization, you may be able to utilize resources from the DoD, the NITTF, or the DSS. One such tool is the PERSEREC Insider Risk Evaluation and Audit Tool. While developed for DoD, it can be applied to most organizations and helps to gauge relative vulnerability to insider threats and adverse behavior. DoD Insider Threat programs may also have access to the Enterprise Program Risk Management tool or EPRM. Contact the DoD Enterprise Program Management Office to learn more.

Screen text: Insider Threat Program Evaluation Plan
Audit Help

Screen text: Select next to continue.

Evaluation Plan - Best Practices
Screen 9 of 12

Narrator: While meeting the minimum standards and policy requirements are essential, truly effective programs also incorporate the lessons of past program best practices and lessons learned. Some examples of best practices include:

- Staying connected with the larger insider threat community to ensure that you are aware of the latest best practices (Consult with DSS, DoD, or NITTF depending on your type of organization);
- Joining working groups and staying up to date with the latest research and publications;
- Consulting with your legal team before implementing new practices, to ensure that they are within your authority and are appropriate relative to privacy or civil liberties concerns;
- Engaging with executive leadership so they understand, advocate for your program, and determine when and how significant activities should be reported to senior management in advance;
- Appropriately sharing insider threat information, both internally and externally, when warranted or required;

- Working with your Public Affairs office prior to disseminating information about the program, its activities, awareness efforts, or training materials developed by the program.

Screen text: Insider Threat Program Evaluation Plan
Best Practices

- Stay connected with the larger insider threat community
- Join working groups
- Consult with legal counsel before implementing new policies and procedures
- Engage with executive leadership and management
- Appropriately sharing insider threat information, both internally and externally when warranted or required
- Consult with Public Affairs when disseminating information externally

Screen text: Select next to continue.

Knowledge Check 1
Screen 10 of 12

Screen text: An Insider Threat Analyst working for an industry program subject to the NISPOM discovered that their organization's employees were being targeted for recruitment by a foreign intelligence entity. The analyst reported the information to the Insider Threat Program Manager and Hub who decided to continue to monitor the situation and gather information.
What other action should the Insider Threat Hub take? Select all that apply.

- Refer the matter to CI.
- Inform the senior leadership.
- Consult with DSS for further actions.
- Report the matter to the NITTF.

Screen text: Select next to continue.

Knowledge Check 2
Screen 11 of 12

Screen text: Regardless of the method used by your Hub to track new policy releases, what step must be followed to assess new policies for possible implications to your program and the organization? Select the best response.

- The legal team must review policy changes prior to incorporating the changes.
- The Program Manager must get buy-in from the workforce prior to incorporating the changes.
- The Hub must review CDSE's Best Practices prior to incorporating the changes.
- The Hub must send the effected SOP's in draft form to the NITTF for approval prior to enacting the changes.

Screen text: Select next to continue.

Lesson Summary
Screen 12 of 12

Narrator: This lesson focused on the management protocols you need to develop to ensure your Insider Threat Hub is ready to handle situations when they arise. We talked about tracking and implementing insider threat policy, establishing formal and informal agreements, integrating an Insider Threat program into the larger organization, and establishing an Insider Threat program Evaluation Plan. Based on the information provide in this lesson, you should be able to describe Insider Threat Hub management protocols.

Screen text: Select Next to view another lesson.

Course Conclusion

Course Summary
Screen 1 of 3

Narrator: As an Insider Threat Hub team member, you will participate in the day to day operations of the Insider Threat Hub. It is critical that you understand the role of Insider Threat programs in protecting classified data, sensitive information, agency infrastructure, and the workforce against internal threats.

Narrator: Your appropriate conduct of Hub functions and activities can make the difference between deterring an insider threat or a loss or compromise affecting national security. This course provided you with an overview of Insider Threat Hub operations including actions conducted to gather, integrate, review, assess, and respond to incidents. These actions accomplish effective deterrence, detection, and mitigation of risks associated with insider threats.

Screen text:
Gather
Integrate
Review
Assess
Respond
Deterrence
Detection
Mitigation of Risks

Screen text: Select Next to continue.

Course Objectives
Screen 2 of 3

Narrator: Congratulations, you have completed the Basic Hub Operations course. You should now be able to perform the listed activities. To receive credit for this course, you must take the Basic Hub Operations examination.

Screen text:
- Given instruction, the student will be able to describe an Insider Threat Hub.
- Given instruction, the student will be able to explain Insider Threat Hub Operations.
- Given instruction, the student will be able to describe Insider Threat Hub management protocols.

Screen text: Select Next to continue.

Course Examination
Screen 3 of 3

Screen text: To receive course credit, you must take the course examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.