Insider Threat Mitigation Responses

Student Guide

April 2024

Center for Development of Security Excellence

Lesson 1: Course Introduction

Introduction

Welcome

While Insider Threat Programs may identify individuals committing espionage or other national security crimes, not all incidents will result in the arrest of a spy. In fact, Insider Threat Programs resolve most cases before they escalate into negative events through the proactive identification of individuals at risk of harming the organization—either wittingly or unwittingly—and the deployment of alternative mitigation options. This allows the Insider Threat Program to protect information, facilities, and personnel—and to retain valuable employees.

Welcome to the Insider Threat Mitigation Responses course! This course describes the ability of multidisciplinary insider threat teams to craft tailored and effective responses to specific behaviors or issues.

Multidisciplinary insider threat teams are comprised of subject matter experts from:

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity
- Behavioral science
- Human resources
- Legal

Case Study

Let's look at the case study of Mark Steven Domingo. Domingo held radicalized extremist views, and frequently created social media and online forum posts advocating for acts of violence and terrorism against religious groups, law enforcement, and military personnel. His ultimate plan was to detonate two homemade improvised explosive devices at a rally in California, with the intent to kill innocent civilians. Fortunately, the FBI was made aware of Domingo's intent through an undercover informant. Teaming with local law enforcement, they were able to intervene and arrest Domingo before he could carry out the potentially deadly terror attack. Domingo was convicted of providing material support to terrorists, and attempted use of a weapon of mass destruction. He was sentenced to 25 years in prison. At his trial, Domingo testified that he was the one who chose to attack the rally, chose to use the bombs, and chose to go through with the plot to commit mass murder. He repeatedly stated that he was intent on killing innocent Americans and would have done so had he not been stopped.

Visit the course Resources to access a printable case study.

Objectives

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

- Explain the role of Insider Threat Programs in mitigating the risks posed by insider threats and how programs mitigate those risks
- Describe factors to consider when formulating a mitigation response to an insider threat incident
- Summarize the ability of multidisciplinary teams to craft mitigation responses tailored to insider threat incidents
- Identify reporting requirements that apply to Insider Threat Programs

Lesson 2: Mitigation Overview

Introduction

Welcome

What would have happened if Mark Domingo's actions were not identified and reported early? An Insider Threat Program can employ alternative response options to mitigate the threat. When identified early, Insider Threat Programs can often resolve common workplace issues, such as interpersonal problems, financial issues, and even disgruntlement or violent tendencies. This results in positive outcomes for both the individual and the organization.

Objectives

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

- Describe the critical pathway model of insider threat and how it applies to mitigating the threat
- Explain the role of Insider Threat Programs in mitigating the risks posed by insider threats and how programs mitigate those risks

The Critical Pathway

Potential Risk Indicators

Domingo's behavior and activities are examples of potential risk indicators (PRIs). PRIs are observable and reportable behaviors and activities that may be exhibited by those at risk of becoming an insider threat. Specific PRIs come from a variety of sources in the security and intelligence communities and may be specific to your organization.

PRIs may converge with adjudicative guidelines for determining eligibility for access to classified information. Some organizations use these to determine insider risk. PRIs generally belong to the categories listed here:

- Access attributes
- Professional lifecycle and performance
- Foreign considerations
- Security compliance and incidents
- Technical activity
- Criminal, violent, or abusive conduct
- Financial considerations

- Substance abuse and addictive behaviors
- Judgment, character, and psychological conditions

Visit the course Resources to access a printable reference of insider threat PRIs.

Behavioral Model of Insider Threat

Dr. Eric Shaw, clinical psychologist and consultant to Federal agencies on insider crime, originated the "critical pathway" model for understanding insider attacks. The components of the model are:

1. Personal Predispositions
2. Stressors
3. Concerning Behaviors
4. Organizational Response
5. Insider Attack

It begins with personal predispositions and stressors, which often correspond to behaviors that emerge as PRIs. Over time, these factors may combine and increase the risk that an individual may become an insider threat.

Consider the Mark Domingo case. While serving in the Army, Domingo displayed difficulty socializing and making friends. He often felt he was being mocked, criticized, and unfairly treated. He was later involuntarily discharged and separated from service on disciplinary grounds. All of this fed directly into his personal stressors. He felt angry, frustrated, and ostracized, and sought an outlet for his negative emotions. These stressors led to concerning behavior by Domingo. He was very active on social media networks, forums, and chatrooms, where he frequently voiced support for violence, religious extremism, and terrorist activity. He actively communicated with others who shared his views and frustrations, and Domingo quickly became self-radicalized and prepared to take violent action. All of these factors culminated in Domingo deciding to detonate two improvised explosive devices at a public rally with the intent to kill as many people as possible. Thankfully, the FBI and law enforcement were able to detect these concerning behaviors, intervene, and prevent a potential disaster.

The model also demonstrates that there are multiple opportunities to redirect individuals from the pathway into more positive behaviors. For example, if Domingo had been off-ramped from a path of radicalization to terrorism, then his behavior may not have escalated. Early intervention can mean the difference between rehabilitation and negative escalation of behavior.

Role of Insider Threat Programs

Overview

Insider Threat Programs fulfill four functions using a holistic approach. First, they help prevent insider threats by providing leadership with threat information that may help to shape decisions about managing insider risk and building resiliency throughout the workforce. Second, they deter

potential insider threats by instituting appropriate security countermeasures, including awareness programs. Next, they detect individuals at risk of becoming insider threats and then finally mitigate the risks associated with those individuals before the issue escalates.

Let's examine these in greater detail.

Prevention, Deterrence, and Detection

Prevention of insider threat actions typically is enabled by ensuring leaders are aware of the current threat landscape, including pertinent insider threat information, activities, and behaviors. This is supported by providing reports and recommendations for threat management and ensuring the workforce understands available resources. Prevention activities complement deterrence.

Deterrence occurs through strategic communications, ensuring personnel are aware of punitive actions that potential offenders may face, and promoting a security posture that detects malicious insider threats. These deterrents support detection.

Detection of PRIs typically occurs through reporting by personnel and monitoring conducted by the program. Once detected, the PRI becomes the catalyst for Insider Threat Program activities, including information gathering, analysis, reporting, and response.

Intervention

The deployment of mitigation options, or your organization's "response" to the insider threat, depends on multiple variables and the unique nature of the insider threat. The mitigation strategy may include referral outside of the Insider Threat Program when required or actions to mitigate the risk internally.

Note that while some insider threat incidents may warrant referrals and intervention from law enforcement, not all meet reporting thresholds or result in an arrest.

In most cases, proactive mitigation responses provide positive outcomes for the organization and the individual. This allows the organization to protect information, facilities, and personnel and to retain valuable employees, and offers intervention to alleviate the individual's stressors and guide them off the critical pathway.

Effective Mitigation

According to the critical pathway model, without intervention, concerning behavior may escalate, causing potential damage to national security, personnel, facilities, or other resources through an insider attack. To be effective, Insider Threat Programs must be attentive to potential issues before they pose a threat, have a risk assessment process in place, address potential issues adequately, and take actions that minimize risk while avoiding those that escalate risk.

Review Activities

Review Activity 1

You receive a report that Ted, an employee in your organization, frequently asks colleagues to loan him money. Ted told one of his colleagues that he has a large gambling problem and a large debt he needs to resolve. Where on the insider threat critical pathway is Ted's situation, based on this report?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Personal Predispositions
- ○ Stressors
- ○ Concerning Behaviors
- ○ All of the Above

Review Activity 2

Which of the following is an effective way to mitigate a potential insider threat based upon what you know about Ted's situation?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Refer Ted to law enforcement
- ○ Tell Ted's colleagues to loan money to him
- ○ Provide him with support and resources to deal with his addiction
- ○ Terminate Ted's employment

Review Activity 3

What functions do Insider Threat Programs perform to reduce the risks posed by insider threats?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Provide leaders with information about the threat landscape
- ☐ Mandate security awareness training for employees
- ☐ Conduct user activity monitoring
- ☐ Document and make available the consequences of insider threat activity

Lesson 3: Response Planning

Introduction

Welcome

Insider Threat Programs must carefully plan their mitigation responses to avoid escalation of risk and to engender a thorough and measured approach to the initiation of punitive action.

Objectives

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

- Identify the primary tenets in responding to insider threat matters
- List possible consequences of inappropriate mitigation responses
- Describe factors to consider when formulating a mitigation response to an insider threat incident

Response Basics

Overview

Insider Threat Programs must follow five primary tenets when planning responses to insider threat incidents, the most important of which is "first, do no harm." Insider Threat programs must also establish and maintain internal procedures and authorities, avoid alerting the individual that they have been identified as a potential insider threat, protect the individual's privacy and civil liberties, and preserve chain of custody and properly handle evidence.

Let's examine these in greater detail.

First, Do No Harm

When an insider threat incident occurs, your Insider Threat Program must carefully assess the situation to avoid exacerbating the situation or increasing risk. Consider whether there is imminent danger to the individual or to others and whether there is an active transmittal of classified information. The Insider Threat Program must thoroughly plan its response before taking action and avoid knee-jerk responses. When planning, communicate and coordinate with your Insider Threat Program team members and other organizational elements.

Establish and Maintain Procedures and Authorities

Your Insider Threat Program must ensure that it has detailed procedures and authorities in place for mitigation response options and should maintain a general response plan that outlines the overall roles and responsibilities of Insider Threat Program personnel and Hub members or other staff and departments.

Avoid Alerting the Individual

In general, your Insider Threat Program should avoid alerting the individual that they have been identified as a potential insider threat. This allows the Program the time needed to determine an appropriate response, ensures the privacy of the individual, and preserves evidence. Note that in some cases immediate intervention may be required.

Protect Privacy & Civil Liberties

Your Insider Threat Program must consider the individual's privacy and civil liberties when developing mitigation response options. Ensure that personal information is properly handled, accessed, used, reported, and retained in accordance with applicable laws, policies, and regulations.

Preserve Chain of Custody and Evidence

Your Insider Threat Program must ensure that early actions taken in incident response do not interfere with the ability of law enforcement or counterintelligence to conduct investigations or operations, or inhibit future prosecution, in cases that require reporting to external agencies. Work with your general counsel and the referral agency to ensure that any evidence associated with the incident is handled properly and adheres to the proper chain of custody.

The *Preserving Investigative and Operational Viability in Insider Threat* course offers additional information if you would like to learn more. You may register for this course through the Center for Development of Security Excellence (CDSE) website.

Unintended Consequences

Impacts

Your Insider Threat Program's response to insider threat indicators or incidents can have long-reaching effects. Even seemingly viable solutions may have inadequate or negative impacts on the individual, on the morale of other personnel, on the mission of your organization, and on public perception of your organization.

Individuals

Possible negative impacts on individuals include disgruntlement due to an overly aggressive response that makes the individual feel poorly treated, which increases risk, and effects to the career or life of the individual due to poor information handling that persists even if the individual is exonerated of wrongdoing or was falsely accused.

Morale

Possible negative impacts on the morale of other personnel include disgruntlement throughout the organization if others learn of an overly aggressive response. This may result in reduced vigilance and hesitancy to report. Overly weak responses may also deter reporting, as it may make personnel feel that it is pointless to report indicators. In addition, seeing a colleague charged with or convicted of a crime, even when it is necessary, may impact morale.

Mission

A possible negative impact on the mission of the organization includes personnel that circumvent the rules to get their work done due to onerous rule or procedure changes at the organization level.

Public Perception

A possible negative impact on public perception of your organization includes low morale and diminished future recruitment capability due to media coverage on the situation and your response.

Threat Analysis

Overview

Insider Threat Programs must take the time to perform the proper gathering and analysis of data before taking action. If an indicator has a plausible explanation and does not increase the risk associated with an individual, an immediate reaction may do more harm than good. Conversely, even if the risk associated with an individual is elevated, it is not necessarily a precursor to a national security crime or act of violence. An immediate response in these instances may compromise the ability of law enforcement and counterintelligence to pursue inquiries, investigations, or operations.

Let's take a closer look at the considerations to keep in mind during threat analysis.

Analysis Goal

The Insider Threat Program should begin by establishing the goal of analysis. What questions is the team trying to answer? State your purpose clearly and in multiple ways to clarify meaning and scope, and consider breaking the problem down into smaller pieces.

For example, consider these large questions that Insider Threat Programs work to resolve:

- Is the individual currently harming the organization's resources?
- If so, is the harm intentional?
- Is there a risk that the individual will do so in the future?

Breaking these into smaller questions can help you to grasp and manage your goal.

When formulating questions, aim to be clear and precise. Anything is possible, so be specific. A clear and precise question might be to consider whether it is possible that the individual stole classified information.

Focus on questions that are significant, answerable, and relevant, such as, "Did the individual have access to the safe? Does the individual display unexplained affluence?"

Finally, differentiate between questions that have a definitive answer, are a matter of opinion, and require consideration of multiple viewpoints. The question, "Were the individual's credentials used to log onto the system on a specific date?" has a definitive answer, while the question, "Was the

individual upset?" is a matter of opinion. While the answer may be relevant and the Program can aggregate the opinions of multiple people to draw a conclusion, the answer is subjective. Also consider whether other viewpoints might reveal a plausible explanation for an indicator. For example, late night activity on an information system may seem suspicious, but the cybersecurity subject matter expert may identify the activity as a common practice of batch patching and updates scheduled to occur when the system is at its lowest usage.

Fair and Balanced Assessment

Insider Threat Programs must also strive toward a fair and balanced assessment of each case. To do so, first identify and acknowledge your assumptions. Consider whether they are justifiable and how they shape your point of view. Next, seek other points of view and evaluate their merits. Finally, ground all claims with the information available. Ensure that your position is supported by the evidence and is based on relevant information. Critically evaluate your position to determine whether you have considered all of the relevant information, whether your conclusion goes beyond the evidence available, and whether there is an argument to be made against your position.

With these considerations in mind, review the example real-world case study below.

Example

Jonathan Toebbe was a nuclear engineer holding the highest levels of national security eligibility, as he had access to highly classified information concerning naval nuclear propulsion, design elements, operating parameters, and performance characteristics. Details of United States nuclear assets and systems are one of our closest guarded secrets, so it's not surprising that they are also the most sought after by adversaries.

In April 2020, Toebbe sent a package to a foreign government containing a sample of Top Secret nuclear reactor data and instructions for establishing a covert relationship to purchase additional Top Secret data. He began corresponding via encrypted email with a representative of the foreign government, who offered Toebbe $100,000 in cryptocurrency if he could provide them with more data. With the help of his wife, Diana, Toebbe continued to secretly deliver stolen Top Secret nuclear data via dead drops to his contact over several months.

Unknown to Toebbe, however, the package he initially sent to the foreign government was intercepted by the United States Embassy and Federal Bureau of Investigation, and his foreign contact was in fact an undercover agent. This initiated the undercover operation that eventually caught him. Both he and his wife were arrested and pleaded guilty to Conspiracy to Communicate Restricted Data, and both were sentenced to over 20 years in prison.

Based on what we've seen in this lesson, what assumptions can be drawn about the Toebbes and their motivations? Are there any possible alternative explanations for their actions?

What do you think the use of stealthy dead drops and requests for cryptocurrency payments might suggest about Toebbe?

How have his actions threatened our national security? Should the FBI have acted sooner considering the category of information involved?

Review Activities

Review Activity 1

Put yourself into the Insider Threat Program at Jonathan Toebbe's organization. In planning a mitigation response to what you have learned about his actions, which of the following should you consider?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ There is an active transmittal of classified information.
- ☐ Toebbe should be notified that he has been identified as a risk.
- ☐ Toebbe's personal information must be properly handled.
- ☐ You should coordinate with law enforcement or counterintelligence to properly handle evidence.

Review Activity 2

How can an Insider Threat Program effectively plan mitigation response options?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Establish the roles and responsibilities for involved personnel on a case-by-case basis
- ○ Act as quickly as possible to minimize how long the risk persists
- ○ Establish procedures, authorities, and a general response plan
- ○ Gather evidence by any means necessary

Review Activity 3

Which of the following is NOT a potential unintended consequence of a failed organizational mitigation response to a possible insider threat?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Poor public perception of the organization
- ○ Reduced employee morale
- ○ Monitoring of organization by federal law enforcement
- ○ Circumvention of rules by personnel due to procedure changes

Review Activity 4

An insider threat incident occurred at your facility. Which of these approaches would support an effective mitigation response?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Act as quickly as possible to put the incident behind your organization.
- ○ Look for the simplest explanation, as this is most likely to be accurate.
- ○ Ask smaller questions to differentiate fact from opinion.

Lesson 4: Multidisciplinary Mitigation Responses

Introduction

Objectives

Multidisciplinary insider threat teams are uniquely positioned to craft mitigation responses tailored to specific insider threat incidents.

Multidisciplinary insider threat teams are comprised of subject matter experts from:

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity
- Behavioral science
- Human resources
- Legal

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

- Differentiate between organizational and individual responses
- Summarize the ability of multidisciplinary teams to craft mitigation responses tailored to insider threat incidents

Types of Responses

Organizational and Individual

Responses to insider threat incidents may be organizational, individual, or both. Organizational responses address a systemic problem with security procedures, training, hiring practices, policies, or other procedures that increase the risk associated with the insider threat. Individual responses address a specific incident and are designed to mitigate the risk associated with or harm caused by a specific individual. In some cases, an organizational response may be effective in addition to or in place of an individual response.

Organizational Response

Examples of organizational responses:

- Changing policy or Standard Operating Procedures (SOP) throughout the organization
- Disabling thumb drives across the organization to prevent downloading sensitive information
- Instituting random bag checks

- Introducing metal detectors
- Providing training or briefings to:
  - Increase awareness of tactics used by adversaries
  - Prevent individuals from becoming unwitting insider threats

Individual Response

Examples of individual responses:

- Internal referrals to human resources or security
- Referral to counterintelligence or law enforcement for inquiry, investigation, or operation
- Referral to counseling, such as mental health or financial
- Punitive actions, such as revocation of access or termination of employment

Tailored Multidisciplinary Mitigation Responses

Overview

The multidisciplinary nature of Insider Threat Programs allows them to craft responses tailored to specific behaviors. A multidisciplinary team working together can provide the most effective responses, which often include a multi-faceted implementation that may include a mix of organizational and individual responses that cover multiple disciplines.

To learn more about the disciplines that comprise a multidisciplinary insider threat team, refer to the *Developing a Multidisciplinary Insider Threat Capability* course. You may register for this course through the Center for the Development of Security Excellence (CDSE) website.

Human Resources (HR)

Example response options specific to human resources:

- Referral to the Employee Assistance Program (EAP) for resources in financial counseling, lending programs, mental health, and other well-being programs
- Medical referrals
- Mediation with supervisors
- Training
- Employee termination procedures
- Other career opportunities

Cybersecurity

Example response options specific to cybersecurity:

- Reduce privileges or system access
- Reconfigure hardware, such as to prevent the use of thumb drives or disc burning
- Limit downloadable file size
- Limit or prevent printing
- Conduct training and awareness campaigns on phishing and other cyber targeting methods
- Increase monitoring

Security

Example response options specific to security:

- Log a security violation or infraction
- Provide security counseling, training, or awareness
- Implement daily bag checks
- Implement random drug and alcohol testing
- Conduct physical monitoring
- Modify Standard Operating Procedures (SOP)

Counterintelligence (CI)

Example response options specific to counterintelligence:

- Referral to the cognizant CI activity for inquiry, investigation, or operation as warranted
- Provide training on foreign targeting methods and recruitment
- Develop a foreign travel brief/debrief program
- Provide threat awareness materials

Law Enforcement (LE)

Example response options specific to law enforcement:

- Referral to the cognizant LE activity for inquiry or investigation as warranted
- Provide criminal threat briefings and awareness materials

Behavioral Science

Example response options specific to mental health and behavioral science:

- Treatment recommendations
- Referral to marital, grief, or other mental health counseling
- Referral to substance abuse rehabilitation programs
- Referral to suicide prevention

Legal

Be sure to include legal in the development of response options to ensure the potential response aligns with privacy protection requirements and other policies.

Monitoring Response

Once the Insider Threat Program implements a mitigation response, it must monitor the response to determine if the risk has been minimized. Note that implementing a mitigation response option does NOT eliminate risk.

Coordinate with your Insider Threat Program partners to determine whether additional mitigation is required. Keep in mind that law or policy may prevent some partners from sharing information with the Program. These may include Employee Assistance Programs, law enforcement, and counterintelligence. As such, the Insider Threat Program should remain vigilant for additional or escalating indicators and document behaviors or activities of concern.

Finally, be sure to periodically re-evaluate the mitigation response to determine if it remains the best option.

Case Study

Recall Mark Steven Domingo, who provided material support to terrorists and attempted to use a weapon of mass destruction. Let's assume for a moment that a colleague, friend, or family member reported Domingo's online activities early on rather than allow his behavior to escalate. What mitigation responses might a multidisciplinary Insider Threat Program have used to proactively redirect Domingo away from the critical pathway?

Some possible mitigation responses that may have applied to the Domingo case include a combination of:

- Referral to counseling resources to help him manage his anger and address depression (individual response; Behavioral Science)
- Monitoring user activities and implementing key word triggers (organizational response; Cybersecurity)
- Instituting daily bag checks within the organization (organizational response; Security)

- Referral to law enforcement for criminal activity, such as threats of violence or preparation to commit a mass attack (individual response; Law Enforcement)
- Referral to counterintelligence for affiliation with known or suspected terrorists (individual response; Counterintelligence)
- Referral to an employee assistance program or termination of employment. Domingo was separated from the Army due to his behavior. His separation did not diminish the risk of him posing a violet threat to others. (individual response; HR)

Note that mitigation responses are not a one-size-fits-all solution. No two insider threat incidents are alike, even when similar potential risk indicators are present, so be sure your team evaluates each incident on a case-by-case basis.

Review Activities

Review Activity 1

For each mitigation response, select whether it is an organizational or individual response. Then check your answers in the Answer Key at the end of this Student Guide.

Referral to counterintelligence or law enforcement

- ○ Organizational
- ○ Individual

Provide threat awareness materials

- ○ Organizational
- ○ Individual

Issue a security violation

- ○ Organizational
- ○ Individual

Terminate employment

- ○ Organizational
- ○ Individual

Offer career path options

- ○ Organizational
- ○ Individual

Provide an Employee Assistance Program

- ○ Organizational
- ○ Individual

Conduct user activity monitoring of information technology systems

- ○ Organizational
- ○ Individual

Referral to mental health counseling

- ○ Organizational
- ○ Individual

Review Activity 2

In the Jonathan Toebbe case study, which of the following disciplines were instrumental in detection and mitigation? Visit Resources to access the case study.

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Law Enforcement
- ☐ Human Resources
- ☐ Counterintelligence
- ☐ Behavioral Science

Lesson 5: Reporting Requirements

Introduction

Objectives

Insider Threat Programs must report certain types of information. This lesson describes reporting requirements for DOD, Federal, and industry Insider Threat Programs.

Here is the lesson objective. Take a moment to review it.

- Identify reporting requirements that apply to Insider Threat Programs

Reporting

Overview

DOD, Federal agency, and industry Insider Threat Programs operate under different regulations and requirements for reporting. When reporting, your Program may need to cease its activities, such as when the referral agency initiates an inquiry or investigation. In other instances, the Program may be able to employ alternate mitigation options concurrent with external actions. Coordinate with the referral agency and your General Counsel to determine the appropriate steps to take after reporting.

Let's examine the reporting requirements for DOD, Federal, and industry Insider Threat Programs in greater detail.

DOD Requirements

DOD Insider Threat Programs are obligated to report certain types of information to:

- The Federal Bureau of Investigation (FBI)
- The DOD Insider Threat Management and Analysis Center (DITMAC)
- The cognizant Military Department Counterintelligence (MILDEP CI) Office

In addition, DOD Insider Threat Programs must report adverse information pursuant to the adjudicative guidelines to information systems such as the Defense Information System for Security (DISS) or other databases as required by the organization. DOD Insider Threat Programs must also report criminal activity to the appropriate military or local law enforcement organization. Finally, the Program must comply with any other internal reporting procedures it has established.

FBI Reporting

Section 811 of the Intelligence Authorization Act requires reporting the to the FBI when classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power. To report to the FBI, use the FBI Headquarters email point of contact for secure reporting or contact your local field office.

Visit the course Resources to access a job aid for Section 811 referrals.

DITMAC Reporting

The DITMAC sets their own reporting thresholds, which are continuously updated based on threats. DITMAC thresholds were published in 2022. When reporting to the DITMAC, use the DITMAC System of Systems (DSOS).

Visit the course Resources to access the current DITMAC reporting thresholds.

MILDEP CI Office Reporting

Enclosure 4 of DOD Directive (DODD) 5240.06, Counterintelligence Awareness and Reporting lists behaviors that DOD entities must report to the MILDEP CI Office, including contacts, activities, indicators, and behaviors related to foreign intelligence, international terrorism, and foreign intelligence entity (FIE) associated cyberspace.

Check your organization's procedures for reporting to your cognizant MILDEP CI Office.

Federal Requirements

Federal Insider Threat Programs are obligated to report to the FBI under Section 811 of the Intelligence Authorization Act when classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power.

In addition, Federal Insider Threat Programs must follow any other internal reporting procedures established within the organization.

Industry Requirements

Industry Insider Threat Programs are obligated to report certain types of information to the FBI and the Defense Counterintelligence and Security Agency (DCSA).

Section 117.8 of 32 CFR Part 117, known as the National Industrial Security Program Operating Manual or "NISPOM rule", requires cleared industry to report actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any location to the FBI and DCSA. The NISPOM rule also requires cleared contractors to report adverse information.

In addition, industry Insider Threat Programs must report via information systems such as DISS or other databases as directed and follow any other internal reporting procedures as established by their Insider Threat Program.

Review Activities

Review Activity 1

For each requirement, select whether it applies to DOD, Federal, and industry Insider Threat Programs. Then check your answers in the Answer Key at the end of this Student Guide.

Report to the FBI when classified information is disclosed in an unauthorized manner to a foreign power

- ☐ DOD
- ☐ Federal
- ☐ Industry

Report to the DITMAC

- ☐ DOD
- ☐ Federal
- ☐ Industry

Report adverse information to DCSA

- ☐ DOD
- ☐ Federal
- ☐ Industry

Review Activity 2

Which would you report under Section 811 of the Intelligence Authorization Act?

Select the best response. Then check your answer in the Answer Key at the end of this Student Guide.

- ○ Authorized disclosure of unclassified information to a foreign government
- ○ Unauthorized disclosure of classified information to a foreign government
- ○ Unauthorized disclosure of classified information to a domestic-owned company
- ○ Authorized disclosure of unclassified documents to a domestic media outlet

Review Activity 3

Which reporting thresholds meet DITMAC requirements?

Select all that apply. Then check your answer in the Answer Key at the end of this Student Guide.

- ☐ Unauthorized disclosure
- ☐ Allegiance to the United States
- ☐ Serious threat
- ☐ Criminal conduct and affiliation

Lesson 6: Course Conclusion

Conclusion

Summary

Insider Threat Programs mitigate the threats posed by witting and unwitting insiders through the deployment of multidisciplinary responses designed to lead the individual away from the critical pathway to becoming an insider threat and reporting information outside of the Program as required.

As you work within your Program to craft tailored and effective mitigation responses, remember that each insider threat incident is unique and should be carefully analyzed and assessed to prevent causing further harm.

Lesson Summary

Congratulations! You have completed the *Insider Threat Mitigation Responses* course.

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

- Explain the role of Insider Threat Programs in mitigating the risks posed by insider threats and how programs mitigate those risks
- Describe factors to consider when formulating a mitigation response to an insider threat incident
- Summarize the ability of multidisciplinary teams to craft mitigation responses tailored to insider threat incidents
- Identify reporting requirements that apply to Insider Threat Programs

To receive course credit, you must take the *Insider Threat Mitigation Responses* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to access the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

You receive a report that Ted, an employee in your organization, frequently asks colleagues to loan him money. Ted told one of his colleagues that he has a large gambling problem and a large debt he needs to resolve. Where on the insider threat critical pathway is Ted's situation, based on this report?

- ○ Personal Predispositions
- ○ Stressors
- ○ Concerning Behaviors
- ⦿ All of the Above (correct response)

Feedback: *Ted's situation falls under all stages of the critical pathway. He has an admitted gambling addiction (personal predisposition), a large debt (stressor), and frequently tries to borrow money from friends/colleagues (concerning behavior).*

Review Activity 2

Which of the following is an effective way to mitigate a potential insider threat based upon what you know about Ted's situation?

- ○ Refer Ted to law enforcement
- ○ Tell Ted's colleagues to loan money to him
- ⦿ Provide him with support and resources to deal with his addiction (correct response)
- ○ Terminate Ted's employment

Feedback: *In Ted's situation, mitigation is best achieved through providing him with support and resources to deal with his addiction.*

Review Activity 3

What functions do Insider Threat Programs perform to reduce the risks posed by insider threats?

- ☑ Provide leaders with information about the threat landscape
- ☑ Mandate security awareness training for employees
- ☑ Conduct user activity monitoring
- ☑ Document and make available the consequences of insider threat activity

Feedback: *These are all examples of functions performed by Insider Threat Programs, including prevention, deterrence, detection, and mitigation.*

Lesson 3 Review Activities

Review Activity 1

Put yourself into the Insider Threat Program at Jonathan Toebbe's organization. In planning a mitigation response to what you have learned about his actions, which of the following should you consider?

- ☑ There is an active transmittal of classified information. (correct response)
- ☐ Toebbe should be notified that he has been identified as a risk.
- ☑ Toebbe's personal information must be properly handled. (correct response)
- ☑ You should coordinate with law enforcement or counterintelligence to properly handle evidence. (correct response)

Feedback: *In assessing the situation, it is necessary to consider the amount of risk, including whether classified information is actively being transmitted. Although you should avoid alerting the individual, it is also still necessary to ensure the subject's privacy and civil liberties are preserved, and that any actions taken by the Insider Threat Program do not hinder later actions by law enforcement or counterintelligence.*

Review Activity 2

How can an Insider Threat Program effectively plan mitigation response options?

- ○ Establish the roles and responsibilities for involved personnel on a case-by-case basis
- ○ Act as quickly as possible to minimize how long the risk persists
- ⦿ Establish procedures, authorities, and a general response plan (correct response)
- ○ Gather evidence by any means necessary

Feedback: *Insider Threat Programs should maintain detailed procedures and authorities for mitigation response options, as well as a general response plan that outlines roles and responsibilities.*

Review Activity 3

Which of the following is NOT a potential unintended consequence of a failed organizational mitigation response to a possible insider threat?

- ○ Poor public perception of the organization
- ○ Reduced employee morale
- ⦿ Monitoring of organization by federal law enforcement (correct response)
- ○ Circumvention of rules by personnel due to procedure changes

Feedback: *The unintended circumstances of a failed mitigation response by an organization can affect the individual, the organization's morale, the mission, and public perception.*

Review Activity 4

An insider threat incident occurred at your facility. Which of these approaches would support an effective mitigation response?

- ○ Act as quickly as possible to put the incident behind your organization.
- ○ Look for the simplest explanation, as this is most likely to be accurate.
- ⦿ Ask smaller questions to differentiate fact from opinion. (correct response)

Feedback: *When performing analysis for a mitigation response, take the time to plan thoroughly, clarify and be specific with your goals, and strive for a fair and balanced assessment of the case.*

Lesson 4 Review Activities

Review Activity 1

Referral to counterintelligence or law enforcement

- ○ Organizational
- ⦿ Individual (correct response)

Feedback: *A referral to counterintelligence addresses a specific incident and aims to mitigate the risk associated with the individual.*

Provide threat awareness materials

- ⦿ Organizational (correct response)
- ○ Individual

Feedback: *Training and awareness campaigns address systemic issues across the organization.*

Issue a security violation

- ○ Organizational
- ⦿ Individual (correct response)

Feedback: *A logged security violation addresses a specific incident and aims to mitigate the risk associated with the individual.*

Terminate employment

- ○ Organizational
- ⦿ Individual (correct response)

Feedback: *Termination of employment is a punitive action that addresses a specific incident and aims to mitigate the risk associated with the individual.*

Offer career path options

- ⦿ Organizational (correct response)
- ○ Individual

Feedback: *A program offering career opportunities is an organizational response.*

Provide an Employee Assistance Program

- ⦿ Organizational (correct response)
- ○ Individual

Feedback: *An Employee Assistance Program is an organizational response.*

Conduct user activity monitoring of information technology systems

- ⦿ Organizational (correct response)
- ○ Individual

Feedback: *User activity monitoring is a way to mitigate risk across the organization.*

Referral to mental health counseling

- ○ Organizational
- ⦿ Individual (correct response)

Feedback: *A referral to mental health counseling aims to mitigate the risk associated with the individual.*

Review Activity 2

In the Jonathan Toebbe case study, which of the following disciplines were instrumental in detection and mitigation? Visit Resources to access the case study.

- ☑ Law Enforcement (correct response)
- ☐ Human Resources
- ☑ Counterintelligence (correct response)
- ☐ Behavioral Science

Feedback: *Toebbe was prevented from disclosing unauthorized information as a result of a multidisciplinary response comprised by counterintelligence and law enforcement. This includes his contact with a foreign country and the resulting investigation by the Federal Bureau of Investigation.*

Lesson 5 Review Activities

Review Activity 1

Report to the FBI when classified information is disclosed in an unauthorized manner to a foreign power

- ☑ DOD (correct response)
- ☑ Federal (correct response)
- ☐ Industry

Feedback: *DOD and Federal Insider Threat Programs must report to the FBI when classified information is or may have been disclosed in an unauthorized manner to a foreign power, per the Intelligence Authorization Act. Industry must report the loss of classified information to DCSA, and espionage, sabotage, or terrorism to both the FBI and DCSA, per the NISPOM Rule.*

Report to the DITMAC

- ☑ DOD (correct response)
- ☐ Federal
- ☐ Industry

Feedback: *DOD Insider Threat Programs must report information that meets DITMAC reporting thresholds to the DITMAC.*

Report adverse information to DCSA

- ☐ DOD
- ☐ Federal
- ☑ Industry (correct response)

Feedback: *Industry Insider Threat Programs must report adverse information as listed in the NISPOM Rule to DCSA.*

Review Activity 2

Which would you report under Section 811 of the Intelligence Authorization Act?

- ○ Authorized disclosure of unclassified information to a foreign government
- ◉ Unauthorized disclosure of classified information to a foreign government (correct response)
- ○ Unauthorized disclosure of classified information to a domestic-owned company
- ○ Authorized disclosure of unclassified documents to a domestic media outlet

Feedback: *Section 811 of the Intelligence Authorization Act concerns the unauthorized release of classified information to foreign powers or agents.*

Review Activity 3

Which reporting thresholds meet DITMAC requirements?

- ☑ Unauthorized disclosure (correct response)
- ☑ Allegiance to the United States (correct response)
- ☑ Serious threat (correct response)
- ☑ Criminal conduct and affiliation (correct response)

Feedback: *All of these thresholds act as a guide for DOD Component Hubs to use when determining whether an incident involved a DOD covered person and should be reported as an insider threat to the DITMAC.*