Supervisor and Command Leader Awareness of Insider Risk

Student Guide

August 2025

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Welcome

Awareness of Insider Risk

Marco, a supervisor, has been hearing more and more about crimes committed by trusted insiders. He knows that leaders, like himself and you, have a responsibility to recognize, address, and mitigate potential risks posed by trusted insiders.

Now, Marco is starting to notice some concerning behaviors from his employee, Liz. He knows she has been plugging her personal phone into her government-issued computer via universal serial bus (USB) cable to charge it, and walking away from her computer with her Common Access Card (CAC) still in the machine.

Although Marco trusts Liz, he also knows that anyone can pose an insider threat risk, whether intentionally or not.

Course Objectives

Welcome to the *Supervisor and Command Leader Awareness of Insider Risk* course. As Liz's supervisor, Marco is in a position where he is likely to be the first to identify her concerning behaviors, and he can be the first to intervene.

Mitigating risk is an ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident. Leaders play a vital role in risk mitigation and can be the first line of defense in detecting, deterring, and mitigating insider threats.

Leaders like you understand the policy and know the proper avenues to reporting and action and are in a unique position to influence their organizational culture and approach insider risk with an eye towards prevention. This course will provide you with information you need to improve your awareness of insider risk and supply you with strategies to mitigate insider risk. Take a minute to review the course objectives.

Course Objectives:

- Analyze scenarios to detect concerning behaviors
- Explain how organizational culture and cultural competency affect the baseline assessment of an individual when considering insider risk
- Assess insider risk scenarios to determine appropriate supervisory actions
- Select appropriate responses to mitigate potential insider threats

Lesson 2: Insider Risk Behaviors

Lesson Introduction

Lesson Objectives

Welcome to the *Insider Risk Behaviors* lesson. Marco needs to decide if Liz's behavior indicates any potential risks so he can choose the best course of action.

Take a moment to review the lesson objectives.

- Explain types of insider threats
- Explain how concerning behaviors become insider threats
- Interpret concerning behaviors and potential risk indicators (PRIs) in a given scenario

Insider Threat Types

Overview

It is essential for government agencies to safeguard classified information, protect national security and individuals, and maintain public trust, not just from the outside, but from the inside as well. To do this, agencies and their leaders need to understand the types of threats posed by trusted insiders.

An insider is any person with authorized access to any U.S. government resources to include personnel, facilities, information, equipment, networks, or systems. This can be through employment, contract, or volunteer activities.

The DOD defines insider threat as the threat that an insider will use her or his authorized access, wittingly or unwittingly, to do harm to the security of the U.S. This includes damage to the U.S. through:

- Espionage
- Terrorism
- Unauthorized disclosure of national security information
- Loss or degradation of organizational resources or capabilities

The National Insider Threat Policy aims to strengthen the protection and safeguarding of classified information by establishing common expectations, institutionalizing executive branch best practices, and enabling flexible

implementation across the executive branch. The DOD Insider Threat Program was established to gather, integrate, review, assess, and respond to information to identify, mitigate, and counter insider threats. This information is derived and identified from:

- Counterintelligence (CI)
- Security
- Cybersecurity
- Civilian and military personnel management
- Workplace violence
- Antiterrorism (AT)
- Risk management
- Other sources

There are many types of insider threats. Let's discuss them now.

Types of Threats

Threats posed by trusted insiders have devastating impacts on:

- National security
- Operations
- Foreign relations
- Government finances
- Long-term strategies

Insider threats can also greatly affect culture, morale, and sense of personal safety. Types of threats include:

- Security violations, such as in the case of Grisel Marrero
- Unauthorized disclosure (UD), such as in the case of Henry Kyle Frese
- National security crimes, such as in the case of Szuhsiung "Allen" Ho
- Workplace violence, such as in the cases of Ivan A. Lopez-Lopez and Mohammad Alshamrani
- Harm to self or suicide
- Sabotage
- Fraud

- Espionage
- Stalking
- Unwitting actions that increase vulnerabilities
- Other counterproductive workplace activities

Insider Threat Categories

All cases of insider threat have far-reaching impacts and fall under two main categories: witting and unwitting.

Witting

Witting actions are those that indicate the individual is aware of their actions and potential threat to critical agency information or infrastructure. Employees can become disgruntled for several reasons, and over time, may choose to act out. Witting insider threats develop over time, usually starting with a significant life event or a series of events that accumulate and lead to a threat.

Unwitting

Unwitting actions are unintentional and unplanned, with no awareness of potential threat indicated by the acting individual. Unwitting insiders may mishandle or accidentally disclose information. They may expose devices to malicious code through phishing scams or by selecting bad links. Insiders may improperly or accidentally dispose of physical records, or even lose data storage devices, such as phones and laptops, by accident or theft.

Awareness of both witting and unwitting insider threats allows agencies to identify vulnerabilities and mitigate risks that could compromise sensitive operations or critical infrastructure.

Case Study: Navy Warship Wi-Fi

Let’s take a look at a real case of a trusted insider who posed a threat by committing a security violation.

In March 2023, former Command Senior Chief Grisel Marrero was convicted and reduced in rank for setting up an unauthorized Wi-Fi system aboard the Navy littoral combat ship USS Manchester. More than 15 Manchester Chief Petty Officers and Marrero were involved in the purchase, installation, and use of the Starlink system aboard the ship. Involved Chief Petty Officers paid Marrero for the system and bought into monthly payment plans for exclusive use of the Wi-Fi.

This conspiracy revealed a months-long effort by involved parties to obtain, install, and conceal the Wi-Fi network from superiors. These efforts included:

- Strategically installing it on the exterior of the ship during a "blanket" aloft period when no exterior documentation would occur
- Falsifying documents
- Lying about the existence of the network when it was detected
- Changing the network name to obscure it

You can learn more about this case and find all of the case studies reviewed in this course in your course Resources.

Review Activity 1: Case Study Activity

In the case of the illegal Wi-Fi aboard the USS Manchester, which statement best describes the behaviors exhibited by Marrero and the other Chief Petty Officers?

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

- ○ Their behaviors were unwitting; Marrero and the Chief Petty Officers did not know installing Wi-Fi on the ship was illegal.
- ○ Only Marrero's behaviors were witting; the Chief Petty Officers were just following Marrero's lead and were unaware of the Wi-Fi policies.
- ○ Marrero and the 15 other Chief Petty Officers' behaviors were witting; their behaviors were intentional and strategic and conducted over a period of months.

How Behaviors Become Insider Threats

Critical Path

As a supervisor, it's important to understand how behaviors—both witting and unwitting—can lead to insider threats.

Shaw and Sellers Critical Path Behavioral Model shows how thought leads to action and how concerning behaviors become inside threats.

Personal predispositions combined with stressors—such as military conflict, political conflict, or economic stress—and concerning behaviors can lead to hostile acts. The stressors in this model can be positive or negative, but the combination of psychological predispositions, stressors, and poor coping strategies can lead to an individual's progression toward posing an insider risk.

For more information about the Shaw and Sellers Critical Path, visit the course Resources.

Personal Predispositions

Personal predispositions include:

- Medical or psychiatric conditions
- Social network risks
- Previous rule violations
- Decision-making deficits

A personal predisposition to substance abuse, a personality disorder, mental illness, or suicidality in combination with behaviors of concern requires a strong organizational response to mitigate risk.

Stressors

Stressors can be personal, financial, or professional. In 78% of UD incidents, individuals experienced at least one negative work-related stressor prior to the unauthorized disclosure (UD), such as a poor performance review, stressful work environment, or interpersonal problems.

Concerning Behaviors

Concerning behaviors are those that are troublesome and could indicate a potential insider threat, often signaling the form an insider's attack may take when it occurs. Concerning behaviors can fall under the categories of:

- Interpersonal
- Technical
- Financial
- Personnel
- Travel
- Mental health
- Social networks

In cases of radicalization, those that demonstrate violent extremist behavior may have unmet needs and view the world through a narrative of personal grievance that is reinforced by a network of like-minded people.

Potential Risk Indicators

Leaders and supervisors contribute to risk mitigation by understanding the Potential Risk Indicators (PRIs) of insider threats and using that knowledge to take appropriate action. Individuals who are at risk of becoming insider threats, and those who ultimately cause significant harm, often exhibit warning signs or indicators. PRIs include a wide range of individual predispositions, stressors, choices, actions, and behaviors. Let's take a closer look at these main PRI categories.

Personal PRIs

Some PRIs and behaviors relate to an individual's personal life. These include financial considerations, substance misuse and alcohol abuse, personal conduct, and criminal conduct.

Financial Considerations

- Inability to satisfy debts
- History of unmet financial obligations
- Evidence of frivolous spending
- Unexplained affluence
- Gambling or tax issues

Substance Misuse and Alcohol Abuse

- Illegal drug use or illegal possession of controlled substances
- Misuse of prescription and non-prescription drugs
- Drug test failures or refusals
- Alcohol-related incidents at or away from work
- Habitual substance or alcohol use

Personal Conduct

- Disruptive, violent, bizarre, or inappropriate behavior
- Family conflict or domestic abuse
- Sexual behavior causing vulnerability
- Emotional or mental instability
- Self-harm, suicidal ideation

Criminal Conduct

- Criminal violent behavior
- Sexual assault and domestic violence
- Weapons-related crimes
- Parole or probation, or violation thereof
- Failure to follow court orders

Professional PRIs

Other PRIs and behaviors take place in the individual's professional environment or place of work. These behaviors are categorized as professional lifecycle and performance, technical activity, or security and compliance incidents.

Professional Lifecycle and Performance

- Lay-offs, furloughs, separations, terminations, demotions, or reprimands
- Leaves of absence or unauthorized absence/AWOL
- Involuntary administrative leave or hardship leave
- Declining performance or poor performance ratings

Technical Activity

- Unauthorized access or use of information technology
- Unauthorized deletion, modification, destruction, or manipulation of electronic records or data
- Unauthorized downloading, storing, or transmitting protected information
- Negligent or lax information technology security practices

Security and Compliance Incidents

- Violations related to the handling of protected information
- Negligent or lax information or physical security practices
- Misuses of information, credentials, access, facilities, or equipment
- Failure to self-report, other non-compliance behaviors

Preferential PRIs

There are also PRIs and behaviors that are related to an individual's beliefs about the U.S. and preferences for foreign nations. These behaviors fall under the categories of allegiance to the U.S., foreign influence and preference, or outside activities.

Allegiance to the U.S.

- Support or advocacy of any acts of sabotage, espionage, treason, terrorism, or sedition against the U.S.
- Association or empathy towards people committing such acts
- Active participation in violent extremist groups
- Divided loyalty

Foreign Influence and Preference

- Foreign travel to countries of concern
- Frequent unofficial foreign travel
- Foreign unofficial contact with foreign intelligence entity (FIE)
- Foreign business, political interests, residency, property, bank accounts, sources of income, passports, or service in foreign government

Outside Activities

- Foreign employment or service
- Concealment to fully disclose outside activities

Escalation Risk Factors

In many cases, individuals exhibit PRIs before committing malicious acts. For example, stalking and suicidal thoughts or ideation are preliminary behaviors that are often evident in cases of mass shootings. In a 2023 United States Secret Service (USSS) report, 36% of mass shooters exhibited stalking or harassment behavior prior to the attack. Similarly, a 2024 study of mass shootings in the U.S. by the Federal Bureau of Investigation (FBI) found that there is current or historic suicidal ideation or intent among 92% of active shooters and 75% of disrupted persons of concern.

One way that leaders and supervisors can explain how PRIs escalate to malicious acts is by understanding the risk factors. Take, for example, suicidal thoughts and

ideation. Approximately 1,200 Americans die by murder-suicide each year, and more than 40% of active shooters die by suicide during the attack. Risk factors include previous suicidal behaviors and current or historical suicidality.

For escalating stalking behavior to violence, risk factors include:

- Having a history of criminality or violence
- Having a relationship with the stalking victim, with up to 41% being known acquaintances
- Presence of damage to personal property of the victim
- Presence of unsolicited gifts or letters

Keep in mind that indicators do not always have diagnostic value or reflect wrongdoing. Indicators are not templates for measuring risk, they are correlations between behavior and potential threats.

Review Activity 2: Scenario Activity

Recall that Liz was charging her phone via universal serial bus (USB) cable in her government laptop and leaving her Common Access Card (CAC) unattended in her machine. How could Liz's behavior pose a threat?

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

- ☐ She could unintentionally degrade the equipment through overuse.
- ☐ She could compromise security of information, either intentionally or not.
- ☐ She could unintentionally cause a data breach.
- ☐ She could unintentionally negatively influence the perception of organizational culture.

Interpreting Concerning Behaviors and PRIs

Overview

Identifying PRIs is not enough to deter or mitigate risk. Leaders and supervisors must be able to recognize and *interpret* concerning behaviors and connect those behaviors to PRIs to analyze potential risk and determine the appropriate actions to take.

Let's study the details of two cases where unmitigated PRIs and concerning behaviors developed into a national security crime and an active shooter incident.

The Importance of Correlating Behaviors with PRIs

In 2017, Szuhsiung “Allen” Ho was sentenced to two years in U.S. prison for violating the Atomic Energy Act. This case falls under the foreign considerations PRI category, which encompasses several behaviors such as:

- Frequent or unreported foreign travel
- Co-habilitation with a foreign national
- On-going contact with a foreign national

Ho’s PRIs include foreign citizenship. Ho was born in Taiwan, then became a naturalized citizen of the U.S. in 1983, holding dual residency in both the U.S. and Taiwan. Frequent foreign travel was another of Ho’s PRIs. Ho lived in Delaware, but spent much of his time in China, fathering a son outside of his marriage in China in 2007. When looking at Ho’s PRIs, it’s important to note that foreign associations and interests may exist for a variety of reasons but rise to a national security concern when they result in divided or conditional U.S. allegiance.

Ho’s concerning behaviors show that he had divided business interests. He owned the Energy Technology International Company in Delaware, but was also employed by China General Nuclear Power Company (CGNPC) as a senior advisor. From 1997 through 2016, Ho conspired to enlist others with development and production of nuclear materials in China without the permission of the Department of Energy, even paying for trips and compensating several U.S. nuclear experts for assisting with the development of nuclear reactor parts in China. This allowed China to quickly develop components for nuclear reactors.

Ho’s concerning behaviors and foreign business interests, in combination with his foreign citizenship and frequent foreign travel PRIs, posed a threat to national security. Ho’s case demonstrates how important it is for leaders and supervisors to correlate behaviors and PRIs to effectively assess and mitigate potential risks.

Unmitigated PRIs and Concerning Behaviors

Unmitigated PRIs and misinterpreted behaviors can escalate to other malicious crimes, including active shooter incidents. Take, for example, the case of SPC Ivan A. Lopez-Lopez who, in April of 2014, open fired in the 49th Transportation Battalion administrative office at Ft. Hood, Texas, injuring 12 soldiers and killing 3 before taking his own life.

The details of the case show he had depression and anxiety associated with a reported traumatic brain injury and possible post-traumatic stress disorder following the death of his mother and grandfather. He had a reported confrontation with other

soldiers over a leave request. Additionally, he was recently transferred and there was a turnover in leadership, resulting in a non-promotion status for Lopez-Lopez, for which he was counseled.

Like other active shooters, the concerning behaviors he demonstrated were observable. In 2014, the FBI published a report titled, *"A Study of Active Shooter Incidents in the United States*," identifying the 21 most common concerning behaviors that are potential risk indicators. Out of those 21, the top 5 included mental health-related issues such as depression, anxiety, paranoia, or other concerns. Also at the top of the list were problematic interpersonal interactions, where individuals experienced more than the usual amount of discord in ongoing relationships with their family. Individuals who posed risks were commonly found to leak their intent to harm others by communicating it to a third-party. They indicated confused or irrational thought processes, demonstrating a change in their quality of thinking and communication. Individuals also demonstrated a decrease in their job performance or unusual or unexplained absences.

Lopez-Lopez exhibited nearly all of these top PRIs and behaviors, but no one intervened, and he carried out the malicious act. Like this case, on average, each active shooter in the study displayed 4 to 5 concerning behaviors over time that were observable to others around them. The most frequent were related to mental health, problematic interpersonal interactions, and talk of violent intent. When others observed concerning behavior, the most common response was to communicate directly to the active shooter—83%— or do nothing—54%. In 41% of cases, it was reported to law enforcement.

When combined with the study, Lopez-Lopez's case shows how knowing PRIs and observing concerning behaviors is not enough to mitigate risk. It is essential for leaders and supervisors to interpret behaviors and connect them with PRIs to determine the appropriate actions to take early on. The report, *"A Study of Active Shooter Incidents in the United States*," can be found in your course Resources.

Review Activity 3: Case Study Activity

Which of the following could be reasonably interpreted as a PRI related to mental health in the Lopez-Lopez case?

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

- ○ He had depression and anxiety, with a reported traumatic brain injury and possible post-traumatic stress disorder following the death of his mother and grandfather.

- ○ He had a confrontation with other soldiers over a leave request.
- ○ He was recently transferred and there was turnover in leadership, resulting in a non-promotion status for Lopez-Lopez, for which he was counseled.

Review Activity 4: Scenario Activity

Which of the following behaviors demonstrated by Liz could be reasonably interpreted as a PRI under the technical activity category?

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

- ☐ Taking a week off of work to travel to Italy with family
- ☐ Responding to emails after work hours
- ☐ Leaving her CAC in the machine unattended
- ☐ Charging her personal phone via USB connected to a government computer

Conclusion

Lesson Summary

You have completed the *Insider Risk Behaviors* lesson.

Lesson 3: Organizational Culture and Cultural Competency

Lesson Introduction

Scenario Introduction

Welcome to the *Organizational Culture and Cultural Competency* lesson.

Marco has been thinking about how Liz was charging her phone through a USB cable connected to her government-issued computer and leaving her CAC in the machine. He recognizes that Liz's behaviors could lead to compromised security of information and potential data breaches. He wants to ensure his response is appropriate. He must consider whether Liz's behavior is based on any cultural misalignments. Marco also needs to consider his baseline understanding of her typical actions and behaviors.

Lesson Objectives

There are both positive and negative impacts of workplace environment and organizational culture on insider risk.

Leaders and supervisors, like you and Marco, are integral to developing and maintaining a positive workplace environment and organizational culture. As a leader, you can rely on your cultural competency to positively impact your organizational culture. By understanding the baseline behaviors of your employees, you can assess potential risks.

Take a moment to review the lesson objectives.

- Distinguish between organizational culture and cultural competence
- Explain how supervisors' cultural competency impacts organizational culture
- Explain how a supervisor uses cultural competency and organizational culture to develop a baseline

Defining Organizational Culture and Cultural Competency

Organizational Culture and Workplace Environment

Organizational culture and workplace environment play an important role in employees' work experiences, both positively and negatively.

Organizational culture refers to the way a company and its employees operate. This includes:

- Communication between different levels of staff
- Employees' perspectives of leadership
- Goals, values, and policies of the organization

Workplace environment is the setting, social features, and physical conditions in which an employee performs their job.

Organizational culture and workplace environment can negatively impact insiders, as was the case with Mohammed Alshamrani, a member of the Royal Saudi Air Force who was participating in a three-year international military training program. On December 19, 2019, Alshamrani shot and killed three American sailors and injured eight others at the Naval Air Station (NAS) in Pensacola, Florida.

The NAS organization failed to adapt to the diversity of its international military community, diminishing its operational effectiveness in a cross-cultural setting. The unprofessional treatment of students by program staff and failure to comply with harassment policies created a negative organizational culture and an adverse work environment. Alshamrani's attack was rooted in anti-American and violent extremist ideology, which was advanced due to the hostile workplace culture.

You can locate this, and other case studies reviewed in this course, in your course Resources.

Cultural Competency

Cultural competency is key in understanding the employees who contribute to the organizational culture and influence the workplace environment. Cultural competence in the workplace refers to an organization's ability to understand and respect diverse cultures, including different nationalities, religions, languages, and ethnicities. Cultural competence allows employees to effectively communicate and collaborate with colleagues from various backgrounds and creates an inclusive work environment.

Leaders and supervisors require cultural competence to choose the appropriate organizational responses. Organizations can achieve cultural competence by constantly evolving in their levels of cultural awareness, cultural knowledge, cultural sensitivities, and functional capacities. Changes in leadership and personnel contribute to fluctuations in an organization's level of cultural competence. Leaders, like you, can demonstrate appropriate organizational responses by:

- Promoting and supporting treatment of psychiatric conditions to help mitigate risk
- Incorporating mental health awareness and resilience training to help the workforce recognize warning signs
- Providing education on the mental health resources available to your employees
- Encouraging open communication and work-life balance policies

Review Activity 1: Case Study Activity

Which of the following best demonstrates the difference between organizational culture and cultural competence in the case of Mohammed Alshamrani?

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

- ○ Organizational culture would have prevented any conflict with U.S. values, while cultural competence would have ensured Alshamrani assimilated better.
- ○ Organizational culture involves creating a psychologically safe environment, while cultural competence would have helped Alshamrani's supervisors recognize and interpret his behaviors within a cultural context.
- ○ Organizational culture would have required Alshamrani to report his feelings, while cultural competence would require the organization to report Alshamrani sooner.

Impacts of Supervisors' Cultural Competency on Organizational Culture

Overview

There are positive and negative impacts of supervisors' cultural competency on organizational culture and, subsequently, insider risk. As is evident in the case of Alshamrani, problematic organizational responses due to inadequate cultural competency can escalate issues and risks.

Problematic organizational responses involve organizations that are inattentive, have no risk assessment process, conduct inadequate investigations, or exhibit other problematic actions. Poor management can exacerbate employee dissatisfaction and counterproductive behaviors that may grow into grievances, espionage, or workplace violence, as was the case with Alshamrani.

Positive organizational responses due to adequate cultural competence lead to fewer negative workplace events. Positive organizational responses involve organizations that promote a positive workplace environment and take a proactive, preventative approach to mitigating issues.

Negative organizational culture and workplace environment impact insider risk through perception, unaddressed stressors, unaddressed toxicity, and unaddressed grievances. Employees who perceive their workplace as unjust are 4.6 times more likely to engage in insider threat behaviors than those who feel their organization is fair and just. Unhealthy disgruntlement, when combined with problematic organizational responses, can be a significant stressor leading to insider threats. Fifty-three percent of employees handle toxic work situations by ignoring or avoiding them, and seventy percent of employees avoid difficult conversations with their boss, colleagues, or direct reports, leaving grievances unaddressed.

Leveraging Cultural Competency

As a supervisor or leader, you are in a unique position to utilize your cultural competencies to positively impact the organizational culture. You can leverage cultural competency by:

- Recognizing the basis for counterproductive or hostile workplace behaviors and grievances
- Recognizing toxic environments
- Understanding cultural differences to change your leadership approach

Recognize the Basis for Behaviors

Counterproductive workplace behaviors cause harm to organizations and individuals through actions such as destruction of property, calling in sick when not ill, stealing, or negative talk. You should ask yourself what is motivating your employees to demonstrate counterproductive workplace behaviors and question if any of the behaviors are related to cultural differences.

Hostile workplace behaviors impact organizations through actions such as sexual or racial harassment, bullying, aggression, victimization, or discrimination. You should ask yourself what the cultural perceptions are of the employees who are demonstrating hostile workplace behaviors and determine what organizational culture or workplace environment factors are influencing their behavior.

Grievances are claims from an employee of adverse impacts due to the misinterpretation or misapplication of a written policy or agreement. These grievances must be addressed by an organization with fairness and in a timely

manner. You should ask yourself how your employees are aligned or misaligned with organizational policies. You should also question if there are any cultural factors preventing your employees from interpreting or applying policy or agreements with fidelity.

Recognize Toxic Environments

You can recognize a toxic environment by acknowledging warning signs, whether they are culturally based or not. You should acknowledge acts or reports of:

- Harassment, abuse, and bullying
- High employee turnover or absenteeism
- Lack of clear purpose and direction
- Risk aversion and fear of failure
- Gossip and conflict
- Micromanagement
- Rivalries and office politics
- Lack of enthusiasm
- Lack of communication regarding people's concerns
- Mistrust of leadership
- Focus on punishment rather than on rewards

Understand Cultural Differences

You can choose more effective approaches to problem-solving and leadership by understanding cultural differences, like, for example, the cultural perception of male and female roles. When a female leader has a male employee who is treating her with disdain or insubordination simply because she is female, she could choose to have a male peer counsel the subordinate employee about appropriate responses to female leadership.

Understanding cultural perceptions can also help you plan your approach to leadership. It may be, for example, very intimidating for a female employee who comes from a culture where men and women don't typically interact in the workplace to have a very involved and collaborative male supervisor. If her supervisor understands her cultural perceptions, he will be able to moderate his approach to leadership and collaborative work.

Scenario: Cultural Competency

Before he decides how to respond to Liz's behavior, Marco will need to consider any cultural differences that Liz may have that could contribute to her behavior.

Marco has known Liz for a long time, and she often shares stories about her early life growing up in Canada and her move to the U.S. when she was a teenager. Her first language is French, and she speaks French on her regular trips to Canada where she visits family. Marco also knows that Liz does not have any religious affiliations, and so he has determined that none of Liz's cultural differences would reasonably explain her concerning behaviors or prevent her from following policies.

Review Activity 2: Scenario Activity

Based on the scenario, how could Marco's cultural competency impact the organizational culture?

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

- ○ Marco could use his cultural competency to shape his employee's negative perceptions of Liz, so they can interpret her behavior as positive as he does.
- ○ Marco's perception of Liz and her cultural background will shape his assessment of her behavior and influence his mitigating actions, which could set expectations for the work unit and affect the broader organizational culture.
- ○ Marco's cultural competency is strong and will help eliminate all bias from the workplace.

Baseline Assessments

Developing a Baseline

Like Marco, you should be aware of abnormal or suspicious behavior as potential indicators that can contribute to an unhealthy work environment, harm to self, or others.

How would you establish what normal behavior is for an employee? Supervisors can develop a reference point for an individual by conducting a baseline assessment, which is a judgement about an individual's character, ethics, and behaviors, based on the individual's previous or typical actions. When an employee is acting "out of character" or differs from their usual baseline behavior, it can be an indicator of potential risk. You can form judgements about an employee's character and ethics to

set expectations for that individual's actions and behaviors by observing and comparing past behaviors with current ones, thus creating a baseline.

Remember, not everyone with off-base behavior poses an insider threat. If you do identify a risk, know that intervention is possible between each phase of the critical path model, and you are well-positioned to intervene.

Scenario: Baseline Assessment

Since Marco has determined that Liz's cultural differences are not likely contributing to her behavior, he must consider what else he knows about her to choose the appropriate response to her behavior.

Marco is thinking about Liz's past behaviors. He knows that Liz has displayed minor behaviors of concern in the past, and he knows that Liz usually follows policies.

Marco is also thinking about the organizational culture. He has only seen one person before Liz display this behavior, which he corrected over a year ago by responding with appropriate actions.

Review Activity 3: Scenario Activity

Which of the following statements describes how Marco can leverage his knowledge about Liz's culture and the culture of the organization to develop a baseline assessment of her?

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

- ○ Marco can reasonably connect Liz's French-Canadian heritage to her concerning behaviors.
- ○ Marco can reasonably conclude that there are little to no effects of her personal culture and the organizational cultures on her behavior. Marco will have to rely on his knowledge of Liz's character, ethics, and typical behaviors to make a baseline assessment.
- ○ Marco can compare Liz's behaviors to previous cases of behaviors within the organization to determine the risk she poses. He will not need to assess her personal baseline behaviors.

Conclusion

Lesson Summary

You have completed the *Organizational Culture and Cultural Competency* lesson.

Lesson 4: Supervisory Impact and Actions

Lesson Introduction

Lesson Objectives

Welcome to the *Supervisory Impact and Actions* lesson.

Now that Marco has a solid baseline understanding of Liz's typical behaviors, he will have to choose how he will assess her concerning behaviors and respond appropriately. Leaders, like you, are in a unique position to identify concerning witting and unwitting behaviors and respond appropriately to reduce insider risk.

Take a moment to review the lesson objectives.

- Explain the impact of supervisors on identifying concerning witting and unwitting insider threat behaviors
- Determine individual and organizational responses available to supervisors
- Choose the appropriate leadership responses to insider risk scenarios

The Impact of Supervisors on Identifying Concerning Behaviors

Overview

As a supervisor or leader, you have a holistic view of your work unit and understand the baseline behaviors of your employees. You can better anticipate behavioral changes based on changes in the organizational culture and workplace environment. You understand that everyone makes mistakes, but you can also spot the difference between willful, purposeful actions and simple mistakes, knowing that multiple mistakes show a pattern of disregard for rules or disdain for authority. You are armed with the understanding of your employees' typical actions and baseline behaviors, and you can identify when an employee's behavior goes against their baseline.

For these reasons, leaders and supervisors can have a big impact on the outcome of an employee's journey down the critical path.

Security and Compliance PRIs

To understand the impact leaders have on identifying concerning behaviors, let's look at a case where a compliance issue resulted in a security threat.

In June 2020, Henry Kyle Frese was sentenced to 30 months in prison for the unauthorized disclosure of classified national defense information (NDI) to two journalists. A news outlet published eight articles containing NDI at the Top Secret level authored by a journalist with whom Frese had a romantic relationship. The details included in the news articles were outside the scope of Frese's job duties. On 30 separate occasions, Frese conducted searches on classified government systems for information regarding the classified topics he discussed with the journalists. Frese transmitted classified NDI related to counterterrorism topics to the journalist using a social media's direct messaging feature. He failed to report suspicious requests from individuals relating to classified national defense information.

Compliance failures like these, whether deliberate or not, are a real security concern. Supervisors and leaders should be aware of security and compliance incidents, including violations related to the handling of protected information, such as unauthorized collection or storage of information or disclosure to unauthorized persons, misuse of facilities or information security privileges, and non-compliance with security training requirements or negligent security practices. A strong understanding of Frese's baseline behaviors and his PRIs may have helped prevent his escalation down the critical path.

You can review this case study and others by accessing your course Resources.

Scenario: Impact of Identifying Concerning Behaviors

Marco has been thinking about how he will respond to Liz's behavior. He notices that Liz has gotten up from her desk and left her phone charging through a USB attached to her computer and has left her CAC in the machine, yet again. He's considering his baseline assessment of Liz and starting to assume her actions are deliberate. Marco decides to wait for Liz to return to her desk and address her. As she returns, Marco overhears her having a conversation with another employee. Liz is asking the employee about classified information that is not essential to her work. Marco now recognizes her concerning behavior is assuredly intentional.

Review Activity 1: Scenario Activity

By being attuned to Liz's baseline and observing her closely, Marco determined Liz's behaviors are witting. Which statement reasonably explains the impact Marco may have on a potential threat situation?

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

- ○ Marco can continue monitoring Liz's behaviors over the next few months to gain compelling information and prove a threat exists.
- ○ Marco can make very little impact, since Liz has already likely committed a crime.
- ○ Marco can now choose to disclose her behaviors with his team to promote awareness of insider threats.
- ○ Marco can now act quickly to choose the appropriate response and mitigate potential insider threat risks.

Choosing Appropriate Responses

Types of Responses

There are different types of individual and organizational responses available to leaders like Marco and you.

Individual responses are targeted at one specific employee, whereas organizational responses are used to target a wide-spread behavior among a group of employees or peers. Individual responses should be based on the individual's behavior, the severity of suspected insider threat, and circumstances surrounding the individual's actions.

Organizational responses should be based on circumstances and organizational culture.

Individual Responses

Leaders can respond by:

- Immediately revoking access to sensitive systems
- Conducting a thorough investigation
- Implementing stricter access controls
- Initiating and exit interview
- Notifying relevant authorities if criminal activity is suspected

- Providing counseling or support (such as offering resources like an employee assistance program (EAP)) if the issue is related to personal stressors
- Reviewing and updating employee security awareness training

Organizational Responses

Leaders can respond by:

- Implementing robust access controls
- Closely monitoring user activities
- Utilizing data loss prevention (DLP) solutions
- Conducting thorough background checks
- Developing an incident response plan
- Educating employees on security policies
- Reviewing employee access levels to identify and address potential risks

Reporting

If you witness suspicious or threatening behaviors and events, you, like all DOD government employees and contractors, are required to report them. Reportable events are those that:

- May influence the status of the entity's or employee's eligibility for access to classified information
- Indicate insider threat to classified information or employees with classified information
- Affect proper safeguarding of classified information
- Indicate classified information has been or is suspected to be lost or compromised

You submit individual culpability reports to the Federal Bureau of Investigations (FBI), and Cognizant security agency (CSA). For cleared defense contractor (CDC) cyber incidents, you report to the Information Security Oversight Office (ISSO), and/or Designated DOD cognizant security office (CSO).

Reporting Procedures

After identifying PRIs, concerning behavior, and/or potential threats, DOD government employees and contractors are mandated to follow reporting procedures and report to their respective insider threat programs.

Incidents meeting specific thresholds must be reported to the Defense Insider Threat Management and Analysis Center (DITMAC) and/or the FBI.

Cleared industry personnel report to the Insider Threat Program Senior Official (ITPSO) or their Facility Security Officer (FSO).

Federal civilian employees must report to their agency's Insider Threat Program, security office, or their supervisor.

Within 72 hours of receiving reported information, security officers, supervisors, and commanders shall forward the information to their organizational counterintelligence (CI) element or their supporting Military Department Counterintelligence Organization (MDCO).

Review Activity 2: Case Study Activity

Frese conducted 30 searches on classified government systems, looking for classified information to share with journalists. If you were Frese's supervisor and became aware of this behavior, what are examples of ways you should respond to this insider risk?

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

- ☐ Immediately fire Frese
- ☐ Report Frese's behavior
- ☐ Encourage employees to communicate and report suspicious behaviors
- ☐ Implement stricter access controls for Frese
- ☐ Revoke Frese's access to sensitive systems

Review Activity 3: Scenario Activity

Now that Marco has identified Liz's behaviors as witting, what should Marco do to respond?

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

- ☐ Write up Liz's PRI as a security infraction and report her behavior

- ☐ Provide Liz with updated security awareness training
- ☐ Revoke or restrict access to sensitive systems
- ☐ Ask Liz to meet with him after work hours to discuss her behavior
- ☐ Take pictures of Liz's desk and email them to his team to ensure Liz's peers understand the security policies

Conclusion

Lesson Summary

You have completed the *Supervisory Impact and Actions* lesson.

Lesson 5: Addressing and Mitigating Risk

Lesson Introduction

Lesson Objectives

Welcome to the *Addressing and Mitigating Risk* lesson.

In situations like that of Marco and Liz, it's critical for supervisors to be able to respond appropriately, proportionally, and swiftly to mitigate potential insider threats. Often, this means supervisors need to anticipate potential risks and have mitigation plans in place. There are proactive engagement strategies that enable supervisors and leaders, like Marco and you, to stay ahead of potential risks and prevent individuals from progressing down critical paths.

Take a moment to review the lesson objectives.

- Explain the supervisor's role in responding to concerning behaviors
- Identify strategies for proactive engagement to prevent individuals from progressing on a critical path

Supervisors' Role in Risk Mitigation

Supervisors at the Frontline

As a supervisor or leader, you are at the frontline of risk mitigation. Most insider threat incidents are preceded by a negative event in the workplace, to which supervisors are most likely privy. Supervisors are often positioned to recognize risk indicators related to professional lifecycles and performance early on. You may detect some potential risk indicators (PRIs) first, such as when an employee:

- Attempts to access information beyond what they "need to know"
- Performs work outside of normal duty hours
- Repeatedly violates security rules and procedures
- Exhibits actions or behaviors associated with disgruntled employees including conflicts with supervisors or coworkers including tardiness, decline in work performance, or unexplained absenteeism
- Shows a change in their mood, makes depressive hopeless statements, or has behavior that raises suicidality concerns

Supervisors' Value and Influence

In addition to early detection capabilities, supervisors have considerable influence and value in risk mitigation. Leaders know the sensitivity and risk level of the positions they manage and have visibility on employee changes. They can maintain an environment where personal conduct, trustworthiness, and character are important, and compliance is not only expected but required. Supervisors take the appropriate action in accordance with agency policy when adverse information regarding an employee is discovered.

Remember, as a leader you have access to resources, such as Human Resources (HR) and Command Directed Behavioral Health Evaluations (CDBHE), that can help guide your risk mitigation actions.

Review Activity 1: Activity

Which of the following statement(s) explain a supervisor's role in responding to concerning behaviors?

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

- ☐ Supervisors attend all regular insider threat trainings and are more knowledgeable about PRIs than their employees.
- ☐ Supervisors have more authority and are more capable of reporting concerning behaviors.
- ☐ Supervisors are positioned to identify risk factors related to professional performance early on and can respond quickly.
- ☐ Supervisors are privy to workplace grievances and can identify PRIs with time to mitigate potential risks.

Proactive Engagement Strategies

Risk Mitigation and Early Detection

In 2010, Petty Officer 2nd Class Bryan Martin was arrested for attempting to sell documents to an individual he believed was a Chinese intelligence officer but who was actually an undercover FBI agent. Martin's PRIs included personal financial problems that were known to his peers, excessive gambling, soliciting of prostitution, and removal of classified documents from secure facilities.

In cases like Martin's where an individual demonstrates PRIs, leaders and supervisors can use proactive engagement strategies to prevent individuals from

progressing on the critical path. Leaders like you can take specific actions to mitigate risk. These actions include:

- Early detection of risk factors
- Relying on existing resources such as HR, counseling, and CDBHE
- Reducing risk of suicide through immediate response

To identify potential risk factors early on, supervisors can:

- Conduct regular security awareness training
- Monitor employee activities for anomalies
- Establish a reporting mechanism for suspicious behavior
- Closely manage privileged access
- Implement strong access controls
- Proactively address employee concerns or grievances

Let's take a look at how you can rely on your resources to reduce risks when you detect them.

Risk Mitigation Resources

To assist with risk mitigation efforts, remember to lean on your existing resources. Your main resources include HR, counseling, and, if available to you, Command Directed Behavioral Health Evaluations (CDBHE). These resources can be instrumental in helping you determine your next steps and can be used in combination with other resources, such as law enforcement or cybersecurity.

Human Resources

HR plays a role in the prevention of insider threats by helping supervisors gain awareness of workplace climate and existing issues. HR can provide valuable insights by filling in gaps of information and providing personnel records, any previously documented medical or psychiatric conditions, previous rule violations or criminal history, or indications of stressors that could indicate a potential risk.

HR can also provide risk mitigation strategies such as offering remedial training and professional counseling, assigning peer mentors, facilitating beneficial transfers, mediation for conflict resolution, providing access to the Employee Assistance Program (EAP) and more.

Counseling

Counseling is a resource supervisors can lean on to assist employees struggling with personal stressors or difficulties receiving the support they need. This is especially helpful in cases where suicidality is suspected.

Command Directed Behavioral Health Evaluations

If available to you, CDBHE exists to provide vital information that can support your risk mitigation efforts.

Disclosures of behavioral health information to a Commanding Officer result because the provider is required to proactively notify the Commander. This is called a “push.” Disclosures also occur because the Commanding Officer has requested the information, which is called a “pull.”

If a Commanding Officer suspects that a behavioral health issue poses a risk to safety or the unit mission, risks can be mitigated by employing either a time-critical evaluation process for emergency situations, or a less critical CDBHE process. A CDBHE will provide a diagnosis, prognosis, safety precautions, administrative recommendations, recommended treatment plan, and determination of fitness for continued duty.

Risk Mitigation and Suicidality

In specific cases where you suspect that someone is contemplating suicide, you can reduce risk by taking both immediate actions and preventative actions.

Immediate Actions

- Find the employee and don’t leave them alone
- Temporarily remove items used to cause self-harm
- Take them to a quiet, private place to have a conversation to determine the next steps
- Make it comfortable to talk about their feelings and state what you know
- Invite the employee to share and show support by listening to them
- Offer hope and help, and don’t challenge or minimize their pain
- If they intend to harm themselves, seek immediate help and alert authorities

Preventative Actions

- Create protective environments that are positive, inclusive, respectful, and supportive
- Send referrals to multidisciplinary teams (MDT) to get guidance and resources
- Educate employees about suicide prevention, including identifying warning signs and supporting suicide loss survivors
- Provide referrals to support services such as Military OneSource, the 988 crisis line, and EAP programs

Engaged Leadership

An engaged leadership is intolerant of violations to dignity and respect, creates an environment of accountability, and provides discipline and praise equitably and fairly.

Proactive engagement strategies for leaders include educating the workforce about risks and resources by suggesting training and informing employees of resources. Leaders can also provide social support by raising awareness about mental health and encouraging a culture where employees feel comfortable seeking support through EAP resources.

Proactive leaders monitor for and address corrosive behaviors that can erode workplace cohesion. They are transparent and upfront about processes and steps regarding concerns. They can reduce help-seeking stigma by promoting a culture that values honesty, trust, respect and policy neutrality. Leaders should normalize sharing and active listening without judgement. Proactive engagement requires leaders to acknowledge disgruntlement and addressing feelings before they evolve into grievances, crises of conscience, or feelings of moral injustice. Engaged leaders know that difficult conversations are crucial for maintaining transparency, resolving conflict, and building mutual trust. To hold employees accountable, leaders can align top-down messaging and provide clear boundaries involving appropriate workplace conduct and hold people accountable.

Finally, proactive engagement includes assessing risks associated with stressors, which starts with identifying workplace aggression and behavioral indicators before it leads to grievances. Engaged leaders model the appropriate actions for those employees who pose risks.

How Leaders Improve Culture

To improve organizational culture, leadership and organizations should engage best practices.

It's important that leaders and supervisors create and commit to a personal code of conduct that aligns their values with that of the organization, and model authenticity in workplace relationships to build trust.

Leaders should focus on clearly communicating values and desired behaviors, linking them to outcomes, and building organizational trust to support the needs of the Insider Threat Programs.

To empower and involve employees, leaders should encourage trust and participation, take action to make employees feel purposeful and respected, and continuously seek and respond to employee feedback.

It's important to support the workforce by building a culture of recognition and developing programs that demonstrate commitment to employee health and well-being.

Finally, to improve the organizational culture, leaders should promote accountability and psychological safety by assuring employees that leadership acts fairly and by demonstrating safety in the reporting process so employes feel secure in prioritizing collective safety over personal consequences.

How Organizations Improve Culture

Organizations have their own set of best practices that can improve organizational culture. It's vital that organizations strive to embed accountability at all levels by tying actions and performance to organizational values.

Organizations should encourage individuals to take responsibility for their actions and consequences. They can foster mutual accountability, where teams develop a collective agenda to enact change and encourage one another to resist being defensive. They should also ensure everyone in the organization works to eliminate discrimination and other unethical practices.

Organizations should also foster a culture of continuous and effective learning. This includes surveying employees and managers to find out skills gaps and training interests, customizing training by focusing on smaller events in shorter timeframes, and sharing training events through team meetings and organization-wide communications.

Review Activity 2: Case Study Activity

Based on Petty Officer 2nd Class Martin's known PRIs of excessive gambling and financial problems, what are some proactive engagement strategies that a supervisor could employ to prevent Martin from progressing down a critical path?

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

- ☐ Encourage Martin's peers to build a friendship with him outside of work and engage him in new hobbies
- ☐ Provide Martin with a raise to help reduce his financial stress
- ☐ Educate Martin and the workforce about resources
- ☐ Encourage a culture where employees like Martin feel comfortable seeking support

Review Activity 3: Scenario Activity

What could Marco have done to prevent Liz from committing concerning witting behaviors?

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

- ○ Marco could have confronted Liz in a team meeting.
- ○ Marco could have addressed Liz's behavior the first time he noticed it, as it was off from her baseline and atypical of her.
- ○ Marco could have requested an emergent evaluation process for this emergency situation.
- ○ Marco could have requested one of Liz's peers to recognize and track Liz's behaviors.

Lesson Conclusion

Lesson Summary

You have completed the *Addressing and Mitigating Risk* lesson.

Lesson 6: Course Conclusion

Conclusion

Course Review

Marco understood the value he had as a supervisor in recognizing, assessing, and mitigating potential threats. He compared Liz's behavior to her baseline, used established reporting paths, and acted early to prevent a threat before it could occur. Just like Marco, you will need to apply the strategies and proactive steps you learned in these lessons to identify concerning behaviors, respond appropriately, and help prevent insider threats within your organization.

Course Summary

Congratulations. You have completed the *Supervisor and Command Leader Awareness of Insider Risk* course.

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

- Analyze scenarios to detect concerning behaviors
- Explain how organizational culture and cultural competency affect the baseline assessment of an individual when considering insider risk
- Assess insider risk scenarios to determine appropriate supervisory actions
- Select appropriate responses to mitigate potential insider threats

To receive course credit, you must take the *Supervisor and Command Leader Awareness of Insider Risk* 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: Case Study Activity

In the case of the illegal Wi-Fi aboard the USS Manchester, which statement best describes the behaviors exhibited by Marrero and the other Chief Petty Officers?

- ○ Their behaviors were unwitting; Marrero and the Chief Petty Officers did not know installing Wi-Fi on the ship was illegal.
- ○ Only Marrero's behaviors were witting; the Chief Petty Officers were just following Marrero's lead and were unaware of the Wi-Fi policies.
- ⊙ Marrero and the 15 other Chief Petty Officers' behaviors were witting; their behaviors were intentional and strategic and conducted over a period of months. (correct answer)

***Feedback**: These behaviors were witting and strategically conducted over a period of several months by Marrero and the other Chief Petty Officers. However, it is unknown from the details provided in the case if the Chief Petty Officers under Marrero felt the need to comply outweighed their ability to refuse buy-in to the network. Although witting, their actions may have been the result of an oppressive organizational culture.*

Review Activity 2: Scenario Activity

Recall that Liz was charging her phone via universal serial bus (USB) cable in her government laptop and leaving her Common Access Card (CAC) unattended in her machine. How could Liz's behavior pose a threat?

- ☐ She could unintentionally degrade the equipment through overuse.
- ☑ She could compromise security of information, either intentionally or not. (correct answer)
- ☑ She could unintentionally cause a data breach. (correct answer)
- ☑ She could unintentionally negatively influence the perception of organizational culture. (correct answer)

***Feedback**: Liz's behavior can pose a threat to security of information, data breaches, and negative perceptions of organizational culture.*

Review Activity 3: Case Study Activity

Which of the following could be reasonably interpreted as a PRI related to mental health in the Lopez-Lopez case?

- ⦿ He had depression and anxiety, with a reported traumatic brain injury and possible post-traumatic stress disorder following the death of his mother and grandfather. (correct answer)
- ○ He had a confrontation with other soldiers over a leave request.
- ○ He was recently transferred and there was turnover in leadership, resulting in a non-promotion status for Lopez-Lopez, for which he was counseled.

Feedback*: Depression, anxiety, and post-traumatic stress disorders are potential risk indicators related to mental health.*

Review Activity 4: Scenario Activity

Which of the following behaviors demonstrated by Liz could be reasonably interpreted as a PRI under the technical activity category?

- ☐ Taking a week off of work to travel to Italy with family
- ☐ Responding to emails after work hours
- ☑ Leaving her CAC in the machine unattended (correct answer)
- ☑ Charging her personal phone via USB connected to a government computer (correct answer)

Feedback*: Leaving a CAC card in the machine and charging her personal phone via USB connected to her government computer are both behaviors that could reasonably be interpreted as technical activity PRIs.*

Lesson 3 Review Activities

Review Activity 1: Case Study Activity

Which of the following best demonstrates the difference between organizational culture and cultural competence in the case of Mohammed Alshamrani?

- ○ Organizational culture would have prevented any conflict with U.S. values, while cultural competence would have ensured Alshamrani assimilated better.
- ⦿ Organizational culture involves creating a psychologically safe environment, while cultural competence would have helped Alshamrani's supervisors recognize and interpret his behaviors within a cultural context. (correct answer)

- ○ Organizational culture would have required Alshamrani to report his feelings, while cultural competence would require the organization to report Alshamrani sooner.

Feedback*: The organizational culture was unable to adapt to the diversity of its international student community and did not promote psychological safety. This was due to a lack of cultural competency amongst leadership since leaders failed to assess the cultural needs of its international student population or interpret behaviors from a cultural lens.*

Review Activity 2: Scenario Activity

Based on the scenario, how could Marco's cultural competency impact the organizational culture?

- ○ Marco could use his cultural competency to shape his employee's negative perceptions of Liz, so they can interpret her behavior as positive as he does.
- ⊙ Marco's perception of Liz and her cultural background will shape his assessment of her behavior and influence his mitigating actions, which could set expectations for the work unit and affect the broader organizational culture. (correct answer)
- ○ Marco's cultural competency is strong and will help eliminate all bias from the workplace.

Feedback*: Marco's perception of Liz and his understanding of her cultural background will impact the way he assesses Liz's behavior and the actions he will take to mitigate risk. Marco's response to Liz's behavior could level-set the expectations for the work unit, thus impacting the organizational culture.*

Review Activity 3: Scenario Activity

Which of the following statements describes how Marco can leverage his knowledge about Liz's culture and the culture of the organization to develop a baseline assessment of her?

- ○ Marco can reasonably connect Liz's French-Canadian heritage to her concerning behaviors.
- ⊙ Marco can reasonably conclude that there are little to no effects of her personal culture and the organizational cultures on her behavior. Marco will have to rely on his knowledge of Liz's character, ethics, and typical behaviors to make a baseline assessment. (correct answer)

- ○ Marco can compare Liz's behaviors to previous cases of behaviors within the organization to determine the risk she poses. He will not need to assess her personal baseline behaviors.

***Feedback**: Marco can reasonably assume that her personal culture is not affecting her behavior, and there is low chance that the organizational culture is affecting her behavior. Marco will have to rely on what he knows about Liz's character, ethics, and typical behaviors to make a baseline assessment of her.*

Lesson 4 Review Activities

Review Activity 1: Scenario Activity

By being attuned to Liz's baseline and observing her closely, Marco determined Liz's behaviors are witting. Which statement reasonably explains the impact Marco may have on a potential threat situation?

- ○ Marco can continue monitoring Liz's behaviors over the next few months to gain compelling information and prove a threat exists.
- ○ Marco can make very little impact, since Liz has already likely committed a crime.
- ○ Marco can now choose to disclose her behaviors with his team to promote awareness of insider threats.
- ⊙ Marco can now act quickly to choose the appropriate response and mitigate potential insider threat risks. (correct answer)

***Feedback**: Because Marco was attuned to Liz's baseline behaviors and was observing her behavior with heightened awareness, Marco was in a position to observe more behaviors in real time. He will be able to take swift action to mitigate potential insider threat risks posed by Liz.*

Review Activity 2: Scenario Activity

Frese conducted 30 searches on classified government systems, looking for classified information to share with journalists. If you were Frese's supervisor and became aware of this behavior, what are examples of ways you should respond to this insider risk?

- ☐ Immediately fire Frese
- ☑ Report Frese's behavior (correct answer)
- ☑ Encourage employees to communicate and report suspicious behaviors (correct answer)
- ☑ Implement stricter access controls for Frese (correct answer)

- ☑ Revoke Frese's access to sensitive systems (correct answer)

***Feedback**: Leaders can respond by reporting behaviors and encouraging their employees to communicate and report suspicious behaviors. Leaders can also respond by implementing stricter access controls and immediately revoking access to sensitive systems.*

Review Activity 3: Scenario Activity

Now that Marco has identified Liz's behaviors as witting, what should Marco do to respond?

- ☑ Write up Liz's PRI as a security infraction and report her behavior (correct answer)
- ☑ Provide Liz with updated security awareness training (correct answer)
- ☑ Revoke or restrict access to sensitive systems (correct answer)
- ☐ Ask Liz to meet with him after work hours to discuss her behavior
- ☐ Take pictures of Liz's desk and email them to his team to ensure Liz's peers understand the security policies

***Feedback**: Marco should write up Liz's technical activity PRI as a security infraction and report her behavior. He should also provide Liz with updated security awareness training. Depending on the frequency of her behavior, Marco can also immediately revoke access to sensitive systems or restrict access controls for Liz.*

Lesson 5 Review Activities

Review Activity 1: Activity

Which of the following statement(s) explain a supervisor's role in responding to concerning behaviors?

- ☐ Supervisors attend all regular insider threat trainings and are more knowledgeable about PRIs than their employees.
- ☐ Supervisors have more authority and are more capable of reporting concerning behaviors.
- ☑ Supervisors are positioned to identify risk factors related to professional performance early on and can respond quickly. (correct answer)
- ☑ Supervisors are privy to workplace grievances and can identify PRIs with time to mitigate potential risks. (correct answer)

***Feedback**: Supervisors are positioned to identify risk factors related to professional performance early on and can respond quickly. Since they are privy to workplace grievances, they can identify PRIs with time to mitigate potential risks.*

Review Activity 2: Case Study Activity

Based on Petty Officer 2nd Class Martin's known PRIs of excessive gambling and financial problems, what are some proactive engagement strategies that a supervisor could employ to prevent Martin from progressing down a critical path?

- ☐ Encourage Martin's peers to build a friendship with him outside of work and engage him in new hobbies
- ☐ Provide Martin with a raise to help reduce his financial stress
- ☑ Educate Martin and the workforce about resources (correct answer)
- ☑ Encourage a culture where employees like Martin feel comfortable seeking support (correct answer)

***Feedback**: Proactive strategies for this case include educating the workforce about resources, encouraging a culture where employees feel comfortable seeking support, and providing Martin with resources like counseling and EAP.*

Review Activity 3: Scenario Activity

What could Marco have done to prevent Liz from committing concerning witting behaviors?

- ○ Marco could have confronted Liz in a team meeting.
- ⦿ Marco could have addressed Liz's behavior the first time he noticed it, as it was off from her baseline and atypical of her. (correct answer)
- ○ Marco could have requested an emergent evaluation process for this emergency situation.
- ○ Marco could have requested one of Liz's peers to recognize and track Liz's behaviors.

***Feedback**: Marco could have addressed Liz's behavior the first time, instead of waiting for more instances of violations to occur.*