

***Developing a  
Multidisciplinary Insider  
Threat Capability  
Student Guide***

March 2024

*Center for Development of Security Excellence*

# Lesson 1: Course Introduction

---

## Introduction

### **Welcome**

Insider threat detection, deterrence, and mitigation resulting in a positive outcome, improves significantly when taking a *multidisciplinary* approach to risk assessment and threat management within an insider threat program.

Consider the case of Machinist Mate Auxiliary Fireman Gabriel Romero, a young man who served in the United States Navy. He had been formally disciplined for tardiness, a minor infraction. While consistent punctuality is associated with most service members, tardiness by some 22-year-olds may be viewed as insignificant, relatively common or normal, and at most a simple inconvenience to their employers. But Romero had also been disciplined for dereliction of duty. At one point, a psychologist identified that Romero was having a phase of life problem, a difficulty related to psychosocial circumstances, and negative family dynamics. He had also been in two motor vehicle accidents within the past year.

These are only some of the indicators of potential risk. When looking at each factor individually, it is possible to understand why one might not initiate an inquiry into Romero. Looking at these factors concurrently, however, provides more context and creates a fuller picture of a person in need of assistance.

On December 4, 2019, Romero reported for patrol duty on the USS COLUMBIA at the Pearl Harbor Naval Shipyard. The shift change and Romero were later described as “ordinary.” As part of his patrol duty, Romero had access to firearms. He took possession of a rifle, a pistol, and 135 rounds of ammunition. Romero began his patrol. When he spotted three civilian employees, he approached them from behind and began firing. All three civilians were lying on the ground when Romero fatally shot himself. Two of the civilians were killed, the third was later released from the local hospital.

While the specific outcome of this case could not have been predicted, *it may have been prevented* by employing a multidisciplinary approach to managing insider risk. The consequences of utilizing a single discipline’s capability, that limits the scope of pertinent insider threat information or places that information into silos, are high. It may even be catastrophic.

### **Objectives**

Welcome to the *Developing a Multidisciplinary Insider Threat Capability* course. This course focuses on the ability of multidisciplinary teams to deter, detect, and mitigate the damage caused by insider threats that may commit acts of workplace violence, sabotage, espionage, and unauthorized disclosure, and how to work effectively in those teams.

Course objectives:

- Determine the role a multidisciplinary capability contributes to an effective Insider Threat Program
- Apply team-building techniques to foster an effective multidisciplinary approach to insider threat matters

If you would like to learn more about Gabriel Romero, refer to the course [Resources](#).

## Lesson 2: Multidisciplinary Capability Overview

---

### Introduction

#### *Objectives*

This lesson describes the purpose of a multidisciplinary insider threat capability and the disciplines that comprise an insider threat team.

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

- State the purpose and goals of a multidisciplinary insider threat capability
- Identify the mission, culture, and policies of each discipline

### Purpose and Goals

#### *Purpose*

While the insider threat is not new, recent cases highlight the need for a more proactive approach to deter, detect, and mitigate the threat associated with trusted insiders. Early identification of concerning behaviors and individuals at risk, and the deployment of appropriate mitigation responses are best accomplished with a multidisciplinary approach that draws on the expertise and resources of each subject matter area.

Federal and DOD policies, including Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information; DOD Directive 5205.16, the DOD Insider Threat Program; and the National Industrial Security Program Operating Manual (NISPOM), require Insider Threat Programs to build a multidisciplinary threat analysis and management capability. These policies are available to you on the [Course Resources](#) page.

Within DOD, the required disciplines include:

- Law enforcement (LE)
- Security
- Counterintelligence (CI)
- Cybersecurity
- Behavioral science, which includes mental health
- Civilian and military personnel management—otherwise known as human resources (HR)
- Legal

## **Goals**

Team members from each discipline work together to monitor, analyze, report, and respond to insider threat matters. The team proactively identifies anomalous behavior that may indicate insiders with threat potential and then deploys mitigation responses that focus on an individual's issues of concern or stressors. When necessary, the team shares relevant information from each discipline with organizational leadership to facilitate timely, informed decision-making and reports information outside the organization as required by policy or regulation.

## **Attaining Goals**

To meet their goals, Insider Threat Programs must use an interdisciplinary approach to program management. This means working collaboratively to:

- Develop the program
- Identify indicators
- Develop training and awareness messaging
- Develop and implement countermeasures
- Respond to incidents

To be effective, team members must:

- Recognize and seek each other's unique perspectives and contributions
- Foster integration among diverse missions and cultures
- Develop a process to coordinate with each other when monitoring, analyzing, responding to, and reporting insider threat matters
- Collectively share information with each other to identify false positives or resolve issues

Note that all processes and procedures must facilitate proper handling, access, use, reporting, and retention of personal information as required by applicable privacy and civil liberties requirements.

## **Disciplines**

### **Overview**

It's not enough to simply bring together subject matter experts from each discipline. To be truly effective, these subject matter experts must function as a team. Strong organizational leadership from your Insider Threat Senior Official and Program Manager is critical throughout the process. But building a team is everyone's responsibility. An important step toward teamwork is to understand each discipline's mission and culture and to realize that

various policies may require each discipline to take certain actions or restrict the actions they can take.

Let's examine these in more detail.

### **Law Enforcement**

LE conducts investigations or criminal intelligence operations that are likely to obtain evidence of a completed crime or the planning of a crime. Their mission is to uphold and enforce criminal laws and to investigate matters so that the judiciary process may be carried out in a fair and impartial manner.

LE's culture is focused on enabling justice and lawfully gathering evidence that may prove or disprove allegations.

Depending on your organization, its actions may be governed by Executive Orders, United States Code, civil and criminal laws and statutes, department and agency regulations, and department and agency memoranda of understanding (MOUs).

<b>Term</b>	<b>Definition</b>
Investigations	Systematic inquiries into an allegation of unfamiliar or questionable activities for the purpose of gathering evidence to substantiate or refute the allegation
Criminal Intelligence Operations	Formalized programs targeting persons or organization whose criminal activity significantly affects the establishment, or those activities designed to gain information of a criminal intelligence nature for law enforcement purposes

### **Security**

Security protects information, technology, physical property and structure, personnel, and other resources. Its purpose is to prevent physical harm, loss of information or technology, and the loss or compromise of personnel, including through preemptive measures such as security education and training.

The culture of security is to act as a shield to protect assets. Traditionally, their actions are referred to as "guns, gates, and guards."

Security actions are governed by these policies: the Federal Information Security Management Act (FISMA), Homeland Security Presidential Directive 12 (HSPD-12), and department and agency regulations, and MOUs for physical security, industrial security, personnel security, and more.

## Counterintelligence

CI systematically collects information about persons or groups that are or may be engaged in harmful activities conducted by or on behalf of foreign entities. CI uses this information to detect, deter, neutralize, and exploit these harmful actions.

If security's culture is to act as a shield, then the culture of CI is to act as the sword that protects secrets and prevents others from spying on us. CI conducts counterintelligence investigations and operations, collects counterintelligence information and acts as a liaison, performs counterintelligence analysis and produces analytic products to articulate the threat, and contributes to CI training and awareness.

Depending on your organization, CI may be bound by the Intelligence Authorization Act; Executive Order 12333, United States Intelligence Activities; the Posse Comitatus Act; and department and agency regulations and MOUs.

Term	Definition
Harmful Activities	These may include: <ul style="list-style-type: none"> <li>• Espionage or other intelligence activities</li> <li>• Sabotage</li> <li>• Terrorism</li> <li>• Assassinations</li> </ul>
Foreign Entities	These may include: <ul style="list-style-type: none"> <li>• Foreign governments or elements thereof</li> <li>• Foreign organizations</li> <li>• Foreign persons</li> <li>• International terrorist activities</li> </ul>

## LE, Security, and CI

LE, security, and CI each focus on some aspect of prevention and protection. These missions overlap and complement one another when deployed effectively. As you strive to understand these disciplines, consider these descriptions.

Discipline	Purpose
Law Enforcement	Capture bad actors
Security	Protect resources from bad actors
Counterintelligence	Identify, prevent, or use bad actors

“Law enforcement wants to identify bad guys and put them in jail. Intelligence wants to identify bad guys and follow them and recruit them, so they can keep getting information from them. These are different cultures...” – Robert Gates, Director of Central Intelligence (1991-1993), Secretary of Defense (2006-2011)

“Counterintelligence investigates the enemy—or if you will in the modern world, the opposition—to learn their capabilities, intentions, methods, and focus. It is not security work. Security protects. It does not attack. CI attacks the actor. It attacks the opposition intelligence structures. It is not speculative. CI feeds security because it helps them focus on meaningful measures and safeguards. Using CI to help security is just smart security.” — Robert Hanssen, Former FBI counterintelligence agent, Soviet spy, and current federal inmate

## **Cybersecurity**

Cybersecurity plans, implements, upgrades, and monitors security measures for the protection of computer networks and information. Part of its mission includes ensuring that appropriate security controls are in place to safeguard digital files and vital electronic infrastructure and responding to computer security breaches and viruses.

Cybersecurity focuses on technical requirements and incidents and their impact on the organization’s mission.

Depending on your organization, its actions may be governed by:

- DOD Instruction (DODI) 8500.01, Cybersecurity
- Presidential Policy Directive 41, United States Cyber Incident Coordination
- FISMA
- National Industrial Security Program Operating Manual (NISPOM)
- A variety of Office of Management and Budget (OMB) memoranda including:
  - M-13-13, Open Data Policy—Managing Information as an Asset
  - M-15-14, Management and Oversight of Federal Information Technology
  - M-16-19, Data Center Optimization Initiative (DCOI)
  - M-16-21, Federal Source Code Policy
  - M-17-05, Fiscal year 2016-2017 Guidance of Federal Information Security and Privacy Management Requirements
  - M-17-06, Policies for Federal Agency Public Websites and Digital Services
  - M-17-09, Management of Federal High Value Assets
  - M-17-15, Rescission of Memoranda Relating to Identity Management

## ***Behavioral Science***

Behavioral science is a broad term that encompasses multiple disciplines that study various aspects of human behavior, including mental health. Behavioral science applies empirical data on human behavior to address issues associated with societal problems, culture, organizational dynamics, interpersonal relationships, mental health, cognition, and substance use.

Many Insider Threat teams include behavioral scientists with expertise in mental health. Mental health addresses the needs of those living with mental illness and promotes overall mental wellness, through individual mental health providers and organizational elements, such as an Employee Assistance Program.

Behavioral science applies a scientific approach to the study of human behavior and its role in complex societal problems, to determine the best intervention strategies to address issues that may arise. Mental health is a critical part of overall wellness, including early identification and intervention for those at risk, with recovery as the goal.

Behavioral scientists who are mental health practitioners are bound by federal laws such as HIPAA, and the Excellence in Mental Health Act, DOD policies concerning the mental health of armed services personnel and substance abuse by DOD personnel, and other policies.

<b>Policy Type</b>	<b>Policies</b>
Federal laws	<ul style="list-style-type: none"> <li>• Health Insurance Portability and Accountability Act (HIPAA)</li> <li>• Excellence in Mental Health Act</li> <li>• Mental Health Parity and Addiction Equality Act of 2008 (MHPAEA)</li> <li>• Section 1034 and 1090a of Title 10, United States Code</li> <li>• Section 711(b) of Public Law 112-81, National Defense Authorization Act for Fiscal Year 2012</li> </ul>
Other policies	<ul style="list-style-type: none"> <li>• Manual for Courts-Martial, United States</li> <li>• National Center for State Courts, Guidelines for Involuntary Civil Commitment</li> </ul>

## ***Human Resources***

Human resources provides centralized and comprehensive personnel data management and analysis for the organization. It manages enterprise-wide programs ranging from recruitment, retention, benefits programs, travel management, language, and culture.

HR establishes a diverse and sustainable workforce to ensure personnel readiness for organizations.

Depending on your organization, DOD, Federal, or even State or local laws and regulations may apply.

Policy Type	Policies
DOD policies	<ul style="list-style-type: none"><li>• DODI 1400.25, DOD Human Resources Activity</li><li>• Privacy Act of 1974</li><li>• DODD 5143.01, Under Secretary of Defense for Intelligence</li><li>• DODD 5124.02, Under Secretary of Defense for Personnel and Readiness</li><li>• DODD 1400.35, Defense Civilian Intelligence Personnel System</li></ul>

### ***Legal***

Legal provides advice regarding all legal matters and services performed within or involving the organization.

It focuses on legal policy and requirements and their impacts.

Policies may include United States Code; the Freedom of Information Act (FOIA); legal standards of conduct and ethics; or other Federal, State, and local statutes as applicable.

## Review Activities

### **Review Activity 1**

Which of the following statements best describes the purpose and goal of a multidisciplinary insider threat capability?

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

- Integrate multiple disciplines to deter, detect, and mitigate insider threats
- Assign individual insider threat matters to specific disciplines for resolution on their own
- Allow Insider Threat Programs physical access to other mission area locations
- Investigate insider threat incidents after they occur

### **Review Activity 2**

*For each question, select the best response. Then check your answers in the Answer Key at the end of this Student Guide.*

Question 1 of 4. Which discipline ensures that security controls safeguard digital files and electronic infrastructure?

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity

Question 2 of 4. Which discipline protects facilities, personnel, and resources from loss, compromise, or destruction?

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity

Question 3 of 4. Which discipline enables a fair and impartial judiciary process?

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity

Question 4 of 4. Which discipline is bound by the Intelligence Authorization Act?

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity

### **Review Activity 3**

Indicate the discipline to which the description applies.

*For each statement, select the best response. Then check your answers in the Answer Key at the end of this Student Guide.*

Provides guidance on legal matters

- Behavioral Science
- Human Resources
- Legal

Focuses on early intervention for those at risk with recovery as the goal

- Behavioral Science
- Human Resources
- Legal

Provides personnel data management and analysis

- Behavioral Science
- Human Resources
- Legal

## Lesson 3: Discipline-Specific Capabilities

---

### Introduction

#### **Objectives**

This lesson describes the capabilities offered by each discipline on a multidisciplinary insider threat team.

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

- Interpret each discipline's insider threat capabilities

#### **Activity**

Based on what you have learned so far, take a moment to consider what role each discipline might play within an Insider Threat Program.

*For each statement, select truth or myth. Then check your answers on the next page.*

Within an Insider Threat Program, the only contribution of law enforcement is to put insider threats in jail.

- Truth
- Myth

Within an Insider Threat Program, the only contribution of security is to take punitive actions against insider threats.

- Truth
- Myth

Within an Insider Threat Program, the only contribution of counterintelligence is to run covert actions against insider threats.

- Truth
- Myth

Within an Insider Threat Program, the only contribution of cybersecurity is to prevent insider threats from accessing information systems.

- Truth
- Myth

Within an Insider Threat Program, the only contribution of behavioral science is to treat mental illness in insider threats.

- Truth
- Myth

Within an Insider Threat Program, the only contribution of human resources is to terminate the employment of insider threats.

- Truth
- Myth

Within an Insider Threat Program, the only contribution of legal is to ensure that the organization does not get sued.

- Truth
- Myth

**Activity Answer Key**

Within an Insider Threat Program, the only contribution of law enforcement is to put insider threats in jail.

- Truth
- Myth (*correct response*)

Within an Insider Threat Program, the only contribution of security is to take punitive actions against insider threats.

- Truth
- Myth (*correct response*)

Within an Insider Threat Program, the only contribution of counterintelligence is to run covert actions against insider threats.

- Truth
- Myth (*correct response*)

Within an Insider Threat Program, the only contribution of cybersecurity is to prevent insider threats from accessing information systems.

- Truth
- Myth (*correct response*)

Within an Insider Threat Program, the only contribution of behavioral science is to treat mental illness in insider threats.

- Truth
- Myth (*correct response*)

Within an Insider Threat Program, the only contribution of human resources is to terminate the employment of insider threats.

- Truth
- Myth (*correct response*)

Within an Insider Threat Program, the only contribution of legal is to ensure that the organization does not get sued.

- Truth
- Myth (*correct response*)

**Feedback:** *These are all myths. Within the context of an Insider Threat Program, the primary focus is on prevention, early detection, and appropriate response.*

## Capabilities

### Overview

The subject matter expertise of each discipline offers unique insights in an insider threat context. Recall that Insider Threat Programs use indicators to identify potential risks and conduct analysis before deploying appropriate responses to mitigate the risk. In addition to these benefits, each discipline also possesses distinct indicators capabilities and mitigation capabilities.

### Law Enforcement

The law enforcement (LE) discipline offers an understanding of criminal behavior and activity, possesses extensive experience in evidence gathering, and understands jurisdiction for successful referral or investigation of criminal activities.

LE can spot indicators related to criminal behavior or activity and, as allowed by policy or regulation, check for violations that occur outside the purview of the organization's security office.

The mitigation capabilities of LE include investigation, arrest, and enabling prosecution or exoneration.

### Security

The security discipline has daily interaction with personnel and can recognize unusual behavior. In addition, security knows the physical layout of the facility and can recommend countermeasures to detect and deter threats.

There are several security disciplines, including physical security, information security, and personnel security, and each of these disciplines may offer unique indicators. However, some general indicators include an individual's:

- Security violations or infractions
- Security posture and behavior
- Compliance with reporting requirements
- Foreign travel or foreign contact information
- Self-reported information related to the adjudicative guidelines or other indicators
- Alteration or removal of classification markings

In response to a potential threat, security may:

- Issue a security violation or infraction
- Provide security counseling, training, or awareness
- Update security policy or procedure, such as requiring limited access to restricted areas
- Conduct end-of-day physical inspection
- Increase physical security capabilities, such as improving lighting

### ***Counterintelligence***

The counterintelligence (CI) discipline offers the ability to access current information about larger threats posed, including:

- Coordinating positive intelligence information from the Intelligence Community (IC)
- Identifying specific threats or targeting from foreign adversaries
- Identifying techniques of targeting and recruitment for proactive awareness
- Developing indicators consistent with prior incidents of espionage or national security crimes

CI can also use a risk-based management approach to help prioritize security countermeasures to defend against threats and vulnerabilities.

CI may be able to look into an individual's foreign associations, contacts, and travel and to identify behavior indicative of use of tradecraft.

Potential mitigation capabilities include:

- Coordinating CI inquiries, investigations, or operations
- Coordinating the development of sources
- Developing countermeasures
- Coordinating referrals to LE or to the IC
- Providing foreign travel briefs and debriefs

### ***Cybersecurity***

The cybersecurity discipline understands the information systems used by the insider, can access user baseline behavior to detect anomalies, and can develop countermeasures and monitoring systems.

Cybersecurity can spot indicators in the results of user activity monitoring (UAM), including unauthorized or unusual access, attempts to circumvent permissions, and the introduction of malware.

In response to an insider threat incident, cybersecurity can remove permissions and access to information systems, increase UAM as permitted by law or regulation, and craft and implement organization-wide changes to information system policies or configuration.

### ***Behavioral Science***

The behavioral science discipline offers an understanding of human behavior that can be used to:

- Identify and refine insider threat indicators and the triggers or user account policies for UAM
- Help develop awareness campaigns and overall marketing and branding of the program, including effective techniques and effects on morale
- Provide a behavioral analysis perspective to mitigation response options, such as how to resolve individual issues or to prevent the escalation of issues
- Assist in team collaboration and de-conflicting information from other disciplines

This discipline may be able to spot behavioral issues in the workplace, understand acts or threats of violence, conduct individual mental health evaluations, and interpret and assess medical files and records.

Its mitigation capabilities include providing treatment recommendations, recommending continued employment or termination, and developing organizational- or individual-level incident responses that take human behavior into account.

### ***Human Resources***

The human resources (HR) discipline has access to direct hires, contractors, vendors, supply chain, and other staffing that may represent an insider threat. HR may also provide an initial screening of all staff. In the HR role, this discipline serves as the policy authority in the workplace, sets the tone and standards for the workplace, and serves as a non-intimidating resource with whom many people are comfortable speaking. HR professionals must also be adept at navigating privacy policy and handling sensitive records and data.

HR may be able to spot indicators from employee assistance referrals and any medical information in the personnel file, including Veterans' Administration or Medicare within DOD Components. HR may also have knowledge of promotions and demotions; conflicts of interest; financial problems, such as liens or wage garnishments; disgruntlement; and issues with the employee's supervisor.

Mitigation capabilities include:

- Setting appropriate employee termination procedures
- Increasing employee satisfaction
- Accessing records and files for inquiries, investigations, or prosecution
- Assessing the need for organizational responses to insider threat incidents

### **Legal**

The legal discipline maintains awareness of legal, privacy, and civil liberties requirements and implements internal policies that adhere to these standards. In addition, legal can coordinate among disciplines for cases that involve CI, legal, and HR entities. In general, legal provides guidance and assurance that the Insider Threat Program's actions are within the law.

Legal ensures that developed indicators meet legal and ethical standards for use and that the Program protects the civil liberties of the individual during mitigation response actions such as internal discipline, referrals to other agencies, or termination of employment.

### **Example**

As you apply what you've learned about each discipline's insider threat capabilities, consider this scenario. A random bag check revealed classified information in Margaret's briefcase. What might each discipline be able to tell you about Margaret?

<b>Discipline</b>	<b>Capability</b>
LE	There is no criminal behavior reported.
Security	Margaret has three previous security infractions for minor events.
CI	Margaret has traveled to a foreign country known to target the information in her briefcase.
Cybersecurity	There is no unusual behavior detected in monitoring, but Margaret has elevated privileges due to her job.
Behavioral Science	Margaret's behavior may indicate that she is suffering from stress.
HR	Margaret notified human resources that she is going through a divorce.
Legal	The random bag check was part of the organization's established security countermeasures and did not invade Margaret's privacy.

## Review Activities

### **Briefing**

In the review activities that follow, consider the following insider threat incident.

*Darren, an employee at your organization, accessed information outside of his need-to-know. What capabilities can a multidisciplinary insider threat team offer in this situation?*

### **Review Activity 1**

*Select the discipline most likely to offer each capability. Then check your answers in the Answer Key at the end of this Student Guide.*

Capability 1 of 4. A security violation will be issued to Darren.

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity

Capability 2 of 4. No prior criminal history has been detected.

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity

Capability 3 of 4. Darren has accessed his organization's information system late at night, when it is inconsistent with his duty hours.

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity

Capability 4 of 4. The information Darren accessed is a high collection priority for an adversary.

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity

**Review Activity 2**

Select the discipline most likely to offer each capability. Then check your answers in the Answer Key at the end of this Student Guide.

Capability 1 of 3. The incident must be documented to demonstrate protection of Darren's civil liberties.

- Behavioral science
- Human resources
- Legal

Capability 2 of 3. Last month, Darren missed three days of work to attend a child custody hearing.

- Behavioral science
- Human resources
- Legal

Capability 3 of 3. Darren may be experiencing stress due to his personal problems.

- Behavioral science
- Human resources
- Legal

## Debriefing

### Overview

Based on the capabilities of the multidisciplinary team, your organization has a more complete picture of what is going on with Darren, and the team may be able to use this information to select a more appropriate response. Discipline-specific capabilities may include:

- Law enforcement: Unauthorized disclosure or other criminal charge, depending on the information accessed and its disposition
- Security: Issue a security violation
- Counterintelligence: Identify potential counterintelligence inquiry, investigation, or operational opportunities
- Cybersecurity: Revisit access procedures and increase security for particular files
- Behavioral science: Recommend treatment for stress, including referral to the Employee Assistance Program or other treatment providers
- Human resources: Provide resources to assist with personal problems
- Legal: Protect privacy and civil liberties

For example, since Darren accessed the files but did not disclose them, he may need to seek counseling to address his stress and receive refresher training on his security responsibilities instead of being charged for unauthorized disclosure or having his employment terminated.

To learn more about mitigation responses to insider threat incidents, refer to the *Insider Threat Mitigation Responses* course available through the Center for Development of Security Excellence (CDSE).

### Case Study

A multidisciplinary insider threat capability may have been able to form a more complete picture of Gabriel Romero to prevent such a tragic event from occurring. Consider the following indicators that were present and how bringing this information together could have made an impact.

Two motor vehicle accidents had been recorded within a year of the incident.

Romero's known risk factors should have prompted an arms, ammunition, and explosives rescreening, in compliance with those standards, potentially preventing him from continuing his post as an armed watchstander.

While CI may not have been involved directly in this case, they might look for factors that show a connection with radicalization to terrorism by foreign terrorist organizations (FTOs) or known or suspected terrorists (KSTs). Romero exhibited displays of anger and withdrawal from shipmates. These may suggest beginnings of radicalization - if and only if there is a link to FTOs or foreign KSTs. This link can be made via social media, internet searches, or other channels. Romero's case, however, was not linked to any FTOs or KSTs.

Proactive user activity monitoring may have detected insight into Romero's behaviors and intentions before escalation.

Mental health providers may have diagnosed and treated Romero's condition, while sharing this information in a way that recognized the chain of command's responsibility in ensuring that high-risk Sailors are identified and provided support, particularly where the Sailor may have access to weapons.

Human resources may have recognized that Romero was under stress due to his difficult family life, connecting the dots to documented performance issues.

Finally, legal could have ensured that sharing of mental health information and any searches were conducted properly so that Romero received the appropriate assistance, remediation, and treatment required.

## ***Lesson 4: Team Coordination and Collaboration***

---

### **Introduction**

#### ***Objectives***

As your multidisciplinary insider threat team begins to form, evolves over time, or replaces members, how can your team coordinate and collaborate effectively?

Every team is unique and will need to decide the processes that work best for their members and circumstances. This lesson discusses techniques that may help you as you plan your team's processes. Keep in mind that your team's needs may change over time, so be open to re-evaluating your team's processes and trying new techniques.

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

- Select techniques to aid team coordination and collaboration

### **Coordination**

#### ***Overview***

As your team decides how members will coordinate with each other, consider the following.

- From a practical standpoint, how will the team communicate?
- Who will lead the team?
- How will the team integrate contributors who are not part of the organization's Insider Threat Program?

Let's examine these considerations in greater detail.

#### ***Communication Logistics***

As your team works to resolve communication logistics, there are two major questions to consider.

The first question is, where are the team members physically based?

Co-located teams are generally considered ideal, as it is easier to meet and talk. This helps team members to get to know each other better and build trust. However, this may not be practical and so team members may be geographically distributed. With appropriate support, even geographically distributed teams can build trust among members to work effectively. For example, consider meeting face-to-face initially so team members can get to know one another before switching to virtual collaboration tools like video conferencing and

SharePoint. To encourage communication and collaboration, demonstrate the benefits of teamwork, such as increased Program effectiveness and gaining new insights.

The second question is, will the team meet face-to-face or virtually?

Face-to-face meetings present logistical issues in bringing everyone together, especially if the team is geographically distributed, but tend to be better for decision making. Virtual collaboration is often good for brainstorming and can be either synchronous or asynchronous.

In synchronous collaboration, team members offer their contributions in real-time through options such as teleconferencing or videoconferencing.

In asynchronous collaboration, team members offer their contributions as their individual schedules permit through tools like SharePoint. It requires greater dedication from the team, but it offers some benefits over face-to-face or synchronous collaboration. For example, asynchronous collaboration can lead to more thoughtful input since contributors can take their time and revise their thoughts. Asynchronous collaboration also provides a written record to better understand a case or to facilitate turnover within the team.

### ***Meeting Purpose and Frequency***

As your team considers when and how often to meet, it's important to realize that the frequency with which you meet should be tied to the purpose of the needed communication.

Most meetings should occur as needed, and so the frequency may vary widely. A multidisciplinary team should consider the following critical items and actions when determining meeting frequency:

- New inquiries
- Case updates
- Case closeout
- Internal process review

Given the many responsibilities of each representative on the team, one may determine that meeting once per week satisfies communication needs. If there are multiple issues to discuss, they may be consolidated into a single weekly meeting. If there are no current cases, then consider meeting quarterly, to remind the team members to report and document case updates regularly, including investigative referrals and after-action reports. Depending on your team's caseload needs, certain meetings may be held on a recurring weekly, monthly, or quarterly basis.

Note that, while these meetings are highly significant to the success of the multidisciplinary insider threat team, so is what happens after those meetings. Post-meeting, ensure that your supervisor or command are provided all necessary feedback and recommendations

determined from the meetings. The team should continue to meet until they determine the risk with the subject is mitigated.

### ***Team Leadership***

The team should have a leader to facilitate collaboration by giving a clear goal, defining measurable objectives and achievement milestones, identifying clear and complementary roles and responsibilities, building relationships with and between team members, setting team norms and expectations, managing conflict within the team, and developing communication protocols and practices. The leader may be appointed by a manager or selected by the team. Note that the team remains accountable for their actions as a group.

### ***External Contributors***

Because not all Insider Threat Programs have a resident subject matter expert from each discipline, the team may need to coordinate with external contributors. Depending on your organization, team members may be able to reach out to:

- Their professional networks
- Other Components, agencies, or companies
- The DOD Insider Threat Management and Analysis Center (DITMAC)
- The National Insider Threat Task Force, which can act as an advisory board on broader policy issues and best practices
- The DOD Behavioral Threat Assessment Center (BTAC) which can assist in prevention and response capabilities for insider threats
- Other similar organizations and working groups for their agency or company

There may also be groups who play a significant role in mitigation response, such as Employee Assistance Programs (EAPs) and training directorates that are not permanent members of your Insider Threat Program but upon whom you rely in the course of your actions.

The team must decide the role that these external subject matter experts will play. For example, they may serve as a reviewer that provides feedback on the team's work, a consultant that provides input and guidance on an as-needed basis, a partner in implementing mitigation response options, or an active participant that performs as a regular team member.

## **Collaboration**

### ***Overview***

Your team must also decide how they will collaborate with one another.

- How will the team ensure mutual understanding?
- How will the team approach tasks?
- And how will the team ensure it truly is multidisciplinary?

Let's examine these in more detail.

### ***Common Framework***

Recall that a multidisciplinary capability is made of disciplines with differing missions, cultures, and governing policies. These differences can lead to fundamental misunderstandings. For example, what do you think of when you think of an inquiry—an informal request for information, a formal questioning or interrogation, or an official investigation? These are all valid definitions that have different implications for insider threat matters.

An agreed upon framework for the team can aid in understanding one another. This may include:

- Collective set of rules, goals, and parameters for conducting insider threat activities
- Toolkit of techniques drawn from each discipline
- Common vocabulary

### ***Approaches***

There are a few approaches the team can take to collaborate. The team may choose to consistently work together jointly, with the team taking collaborative ownership of all elements. The team may also choose to divide tasks among team members, with individuals taking ownership of various elements. Many teams collaborate using a mix of these approaches.

The approach your team uses will largely depend on the preferences and comfort level of your team, but note that no matter which approach your team uses, the team as a whole is still accountable.

### ***Multidisciplinary Teamwork***

As your team works to fulfill its mission, it will deal with some complex questions, such as:

- What threat does this person pose?
- How can we mitigate the threat?

As the team works toward answers to these questions, consider the interdisciplinary implications and break the questions down further. For example, the team may want to ask themselves:

- What are the disciplines inherent in this question?
- Are we dealing with all of the relevant disciplines in this question?
- Are we leaving out some important disciplines?

The team should include all disciplines, even if it may not seem relevant. For example, consider the following scenario. Recall the incident with Margaret, who was found with classified information in her briefcase during a random bag check.

After determining whether the activity meets the threshold for reporting, the team at your organization considers what Margaret's motivation and intent behind having the classified information was. *Was this intentional illicit activity?*

When breaking this question down, each discipline has questions of its own that help to develop a holistic view of Margaret and her possible motives for having the information.

Discipline	Question(s)
LE	Does Margaret have a history of criminal behavior?
Security	Does Margaret have a history of security infractions?
CI	Does Margaret have any connections to persons or places that would have interest in the information?
Cybersecurity	Does Margaret demonstrate unusual use of information systems? What privileges does she have?
Behavioral Science	What does Margaret's personal behavior indicate?
HR	Does Margaret have any life changes occurring?
Legal	Was the search lawful?

## Review Activity

### ***Review Activity***

*Select the best response to each question. Then check your answers in the Answer Key at the end of this Student Guide.*

Question 1 of 4. Which technique would you recommend to a multidisciplinary team that lacks clear goals, roles, and communication protocols?

- Develop a common framework
- Select a team leader
- Meet face-to-face
- Bring in an external subject matter expert

Question 2 of 4. Which technique would you recommend to a multidisciplinary team that frequently misunderstands one another?

- Develop a common framework
- Select a team leader
- Meet face-to-face
- Bring in an external subject matter expert

Question 3 of 4. Which technique would you recommend to a multidisciplinary team that is missing a discipline?

- Develop a common framework
- Select a team leader
- Meet face-to-face
- Bring in an external subject matter expert

Question 4 of 4. Which technique would you recommend to a multidisciplinary team that is co-located and must make an important decision?

- Develop a common framework
- Select a team leader
- Meet face-to-face
- Bring in an external subject matter expert

# Lesson 5: Problematic Team Dynamics

---

## Introduction

### Overview

On any team, differences of opinion are inevitable. This is especially true for multidisciplinary insider threat teams, where the biggest failures often center on information sharing. By design, the members of these teams come from different backgrounds, hold different viewpoints, and have different perspectives. In addition, the team exists to deal with complex, high-stakes issues.

Too much conflict can lead to team breakdown. Conversely, too much focus on consensus can lead to dysfunctional decision-making. Teams should strive for an open discussion and exchange of ideas. This lesson examines these concepts.

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

- Recognize problematic team dynamics and select techniques to manage them

## Artificial Consensus

### Types

The nature of group dynamics and the desire for agreement may lead to problematic decision making, such as premature consensus, groupthink, or group polarization.

- **Premature consensus** is settling on a less-than-optimum solution because everyone can agree. For example, an insider threat awareness or communications plan that is generic and not tailored to the workforce.
- **Groupthink** is inadequate critical evaluation of a solution in order to promote consensus and minimize conflict and leads to stagnation and complacency. For example, failure to evaluate and dynamically evolve elements of the Insider Threat Program, such as training and user activity monitoring, after the original implementation.
- **Group polarization** is the tendency for groups to arrive at a solution that is more extreme than the average group member's personal position. For example, instituting mandatory daily bag checks without considering the impact on the organization's mission in relation to actual enhancement of security or unintended consequences.

## ***Techniques***

To combat artificial consensus, encourage participation from all members, including alternate viewpoints, and limit the ability of a few to dominate discussion. These may help to identify overt or unconscious bias. Keep discussion moving. Be prepared to table issues when necessary to avoid getting stuck on an issue. Develop a variety of potential options before exploring any one in depth. Be sure to examine potential negative aspects and consequences of each option before making a decision.

## **Managing Conflict**

### ***Overview***

Conflict is not necessarily disruptive. When properly managed, it can lead to productive solutions. There are two primary ways teams can manage conflict:

- First, team members should strive for an exploratory mindset rather than an advocacy mindset.
- Second, team members should agree to practice adversarial collaboration.

Let's examine these in greater detail.

### ***Mindset***

With an advocacy mindset, team members engage in a contest where the purpose of discussion is to lobby for a specific solution. It frames participants as spokespeople who strive to persuade others, defend their positions, and downplay weaknesses. With an advocacy mindset, team members tend to discourage or dismiss minority views, and there are losers and winners in the outcome.

With an exploratory mindset, team members engage in collaborative problem solving where the purpose of discussion is to test and evaluate solutions. It champions participants as critical thinkers who present balanced arguments, remain open to alternatives, and accept constructive criticism. With an exploratory mindset, team members cultivate and value minority views and possess collective ownership over the outcome.

Team members should try to maintain an exploratory mindset when collaborating.

### ***Adversarial Collaboration***

Adversarial collaboration is an agreement between opposing parties on how they will work together to resolve or gain a better understanding of their differences. When both sides are open to discussion, it can aid in seeing the merit of the other person's perspective.

Approaches to adversarial collaboration include:

- A key assumptions check

- An analysis of competing hypotheses
- The Nosenko approach
- Argument mapping
- Mutual understanding
- Joint escalation

### **Key Assumptions Check**

In a key assumptions check, each side notes the assumptions used in their mental models and then they discuss each assumption, focusing on the rationale behind it and how it might be refuted or confirmed.

A key assumptions check can be helpful when weighting the values of behaviors in risk equations or other analytic methods. For example, insider threat team members may believe that some sources of information, such as user activity monitoring or security violations, are more meaningful or valuable.

### **Analysis of Competing Hypotheses**

In an analysis of competing hypotheses, both parties agree on a set of hypotheses and then rate each item as consistent or inconsistent with each hypothesis. Unresolved differences generally point to unrecognized assumptions or alternate rationale for differing interpretations.

This approach can be useful when determining the best overall communications and messaging plan within the organization for the Insider Threat Program.

### **Nosenko Approach**

In the Nosenko approach, which is related to the analysis of competing hypotheses, each side identifies items that they believe are of critical importance and must address each of these items.

This approach is best employed when developing an implementation plan.

### **Argument Mapping**

In argument mapping, both sides agree to map the logical relationship between each element of an argument in a single map. The argument map should include the rationale for and against a given conclusion.

Argument mapping can be useful when determining organization-specific indicators that must be reported to the Insider Threat Program.

**Mutual Understanding**

In a mutual understanding approach, each side explains the other's perspective to a neutral third party.

It can be useful for resolving conflicts over competing mitigation response options.

**Joint Escalation**

In joint escalation, team members must prepare a joint statement explaining the disagreement to their superiors in order to escalate an issue. This requires team members to give additional consideration to the other's perspective and allows managers to receive multiple perspectives on the conflict, its causes, and possible resolutions.

Joint escalation can be useful in determining internal policies, procedures, roles, and responsibilities of team members.

## Review Activities

### Review Activity 1

Are the team dynamics listed below problematic?

*For each statement, select Yes or No. Then check your answers in the Answer Key at the end of this Student Guide.*

Mary and Len disagree on a mitigation response option and list the pros and cons of each.

- Yes
- No

Jake and Samantha present two options to the rest of the team and then take a vote.

- Yes
- No

The team bans all removable media without exception following the loss of information.

- Yes
- No

### Review Activity 2

*For each question, select the best response. Then check your answers in the Answer Key at the end of this Student Guide.*

Question 1 of 4. Which technique would you use to avoid group polarization?

- Brainstorm potential consequences of an option
- Engage in an exploratory mindset
- Explain each other's perspective to a third party
- Use a key assumptions check

Question 2 of 4. Which technique would you use to enhance collaborative ownership of a solution?

- Brainstorm potential consequences of an option
- Engage in an exploratory mindset
- Explain each other's perspective to a third party
- Use a key assumptions check

Question 3 of 4. Which technique would you use to resolve the relative importance assigned to pieces of information?

- Brainstorm potential consequences of an option
- Engage in an exploratory mindset
- Explain each other's perspective to a third party
- Use a key assumptions check

Question 4 of 4. Which technique would you use to clear a misunderstanding between two team members?

- Brainstorm potential consequences of an option
- Engage in an exploratory mindset
- Explain each other's perspective to a third party
- Use a key assumptions check

## Lesson 6: Course Conclusion

---

### Conclusion

#### Summary

In this course, you learned the capabilities of an effective multidisciplinary insider threat team. Let's take a look at an example of what one of these teams can accomplish when working together.

Christopher Paul Hasson was a trusted insider as a Lieutenant in the United States Coast Guard. He had Secret clearance, but was denied Top Secret Sensitive Compartmented Information (TS/SCI). Internet searches, emails, text messages, and saved documents revealed violent extremist ideology. Hasson self-identified as a "White Nationalist" for over 30 years. He purchased illegal drugs from Mexico online and took them while at work. Search warrants revealed illegal weapons, silencers, tactical gear, pills, and more.

Take a moment to consider how each discipline might have contributed to the prevention of one or more intended terrorist attacks in this case. For each item, which discipline might have been able to contribute to the multidisciplinary insider threat team?

Hasson's career as a US Coast Guard lieutenant was tracked by HR. While Hasson self-identified as a White Nationalist, during his career he did not present as violent, racist, or anti-equality. His peers would not have described him as White Nationalist. In Hasson's case, more than HR was needed to detect a potential threat, underscoring the need for multidisciplinary teams.

The denial of TS/SCI level clearance might have been noted by security.

His violent extremist views may have been noted by behavioral science, while counterintelligence would have screened for extremist activities tied to foreign entities.

Cybersecurity picked up on his concerning and illegal activities on U.S. government systems, including illegal drug purchasing – alerting legal to issue a search warrant, which was conducted by law enforcement.

The Christopher Paul Hasson case was an example of a positive insider threat outcome in that an insider threat hostile act was prevented by an effective insider threat program. The case highlighted a holistic approach and the successful collaboration between the organization's insider threat program and other agencies. Hasson was arrested and pled guilty to weapons and drug charges. He was sentenced to 160 months in prison.

Refer to the job aid in the course [Resources](#) for additional information about the Hasson case.

**Lesson Summary**

Congratulations! You have completed the *Developing a Multidisciplinary Insider Threat Capability* course.

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

- Determine the role a multidisciplinary capability contributes to an effective Insider Threat Program
- Apply team-building techniques to foster an effective multidisciplinary approach to insider threat matters

To receive course credit, you must take the *Developing a Multidisciplinary Insider Threat Capability* examination. Please use the STEPP system from the Center for Development of Security Excellence to register for the online exam.

# Appendix A: Answer Key

---

## Lesson 2 Review Activities

### Review Activity 1

Which of the following statements best describes the purpose and goal of a multidisciplinary insider threat capability?

- Integrate multiple disciplines to deter, detect, and mitigate insider threats (*correct response*)
- Assign individual insider threat matters to specific disciplines for resolution on their own
- Allow Insider Threat Programs physical access to other mission area locations
- Investigate insider threat incidents after they occur

**Feedback:** A multidisciplinary insider threat capability is meant to proactively detect, deter, and mitigate potential insider threats through early identification and deployment of appropriate mitigation responses.

### Review Activity 2

Question 1 of 4. Which discipline ensures that security controls safeguard digital files and electronic infrastructure?

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity (*correct response*)

**Feedback:** Cybersecurity ensures that appropriate security controls are in place to safeguard digital files and vital electronic infrastructure.

Question 2 of 4. Which discipline protects facilities, personnel, and resources from loss, compromise, or destruction?

- Law enforcement
- Security (*correct response*)
- Counterintelligence
- Cybersecurity

**Feedback:** Security protects facilities or installations, personnel, and resources and capabilities from loss, compromise, and destruction.

Question 3 of 4. Which discipline enables a fair and impartial judiciary process?

- Law enforcement (*correct response*)
- Security
- Counterintelligence
- Cybersecurity

**Feedback:** *LE investigates matters so that the judiciary process may be carried out in a fair and impartial manner.*

Question 4 of 4. Which discipline is bound by the Intelligence Authorization Act?

- Law enforcement
- Security
- Counterintelligence (*correct response*)
- Cybersecurity

**Feedback:** *CI is bound by the Intelligence Authorization Act.*

### **Review Activity 3**

Provides guidance on legal matters

- Behavioral Science
- Human Resources
- Legal (*correct response*)

**Feedback:** *Legal provides advice regarding all legal matters and services performed within or involving the organization.*

Focuses on early intervention for those at risk with recovery as the goal

- Behavioral Science (*correct response*)
- Human Resources
- Legal

**Feedback:** *One component of behavioral science is mental health, including early identification and intervention for those at risk, with recovery as the goal.*

Provides personnel data management and analysis

- Behavioral Science
- Human Resources (*correct response*)
- Legal

**Feedback:** HR provides centralized and comprehensive personnel data management and analysis for the organization.

## Lesson 3 Review Activities

### Review Activity 1

Capability 1 of 4. A security violation will be issued to Darren.

- Law enforcement
- Security (*correct response*)
- Counterintelligence
- Cybersecurity

**Feedback:** Security has the ability to issue security violations and infractions.

Capability 2 of 4. No prior criminal history has been detected.

- Law enforcement (*correct response*)
- Security
- Counterintelligence
- Cybersecurity

**Feedback:** LE has the ability to check for violations outside of the organization.

Capability 3 of 4. Darren has accessed his organization's information system late at night, when it is inconsistent with his duty hours.

- Law enforcement
- Security
- Counterintelligence
- Cybersecurity (*correct response*)

**Feedback:** Cybersecurity has the ability to check for indicators derived from user activity monitoring (UAM).

Capability 4 of 4. The information Darren accessed is a high collection priority for an adversary.

- Law enforcement
- Security
- Counterintelligence (*correct response*)
- Cybersecurity

**Feedback:** *CI can provide information on foreign threats and targeting.*

### **Review Activity 2**

Capability 1 of 3. The incident must be documented to demonstrate protection of Darren's civil liberties.

- Behavioral science
- Human resources
- Legal (*correct response*)

**Feedback:** *Legal ensures the protection of individuals' civil liberties during mitigation response actions.*

Capability 2 of 3. Last month, Darren missed three days of work to attend a child custody hearing.

- Behavioral science
- Human resources (*correct response*)
- Legal

**Feedback:** *Human resources has access to information about personnel.*

Capability 3 of 3. Darren may be experiencing stress due to his personal problems.

- Behavioral science (*correct response*)
- Human resources
- Legal

**Feedback:** *Behavioral science may be able to pinpoint a cause underlying a behavioral issue.*

## Lesson 4 Review Activity

### **Review Activity**

Question 1 of 4. Which technique would you recommend to a multidisciplinary team that lacks clear goals, roles, and communication protocols?

- Develop a common framework
- Select a team leader (*correct response*)
- Meet face-to-face
- Bring in an external subject matter expert

**Feedback:** *A team leader can aid collaboration by giving a clear goal for the team, identifying roles and responsibilities, and developing communication protocols.*

Question 2 of 4. Which technique would you recommend to a multidisciplinary team that frequently misunderstands one another?

- Develop a common framework (*correct response*)
- Select a team leader
- Meet face-to-face
- Bring in an external subject matter expert

**Feedback:** *An agreed upon common framework can aid in understanding.*

Question 3 of 4. Which technique would you recommend to a multidisciplinary team that is missing a discipline?

- Develop a common framework
- Select a team leader
- Meet face-to-face
- Bring in an external subject matter expert (*correct response*)

**Feedback:** *When a multidisciplinary team does not have a resident subject matter expert from each discipline, the team may need to seek out external contributors.*

Question 4 of 4. Which technique would you recommend to a multidisciplinary team that is co-located and must make an important decision?

- Develop a common framework
- Select a team leader
- Meet face-to-face (*correct response*)
- Bring in an external subject matter expert

**Feedback:** *Face-to-face meetings tend to be better for decision-making.*

## Lesson 5 Review Activities

### Review Activity 1

Are the team dynamics listed below problematic?

Mary and Len disagree on a mitigation response option and list the pros and cons of each.

- Yes
- No (*correct response*)

**Feedback:** *Mary and Len demonstrate exploratory mindsets and are engaged in adversarial collaboration.*

Jake and Samantha present two options to the rest of the team and then take a vote.

- Yes (*correct response*)
- No

**Feedback:** *Jake and Samantha demonstrate advocacy mindsets, are dominating the rest of the team, and limit the ability of the team to develop additional options.*

The team bans all removable media without exception following the loss of information.

- Yes (*correct response*)
- No

**Feedback:** *This is an example of group polarization.*

**Review Activity 2**

Question 1 of 4. Which technique would you use to avoid group polarization?

- Brainstorm potential consequences of an option (*correct response*)
- Engage in an exploratory mindset
- Explain each other's perspective to a third party
- Use a key assumptions check

**Feedback:** *Group polarization often fails to consider unintended consequences.*

Question 2 of 4. Which technique would you use to enhance collaborative ownership of a solution?

- Brainstorm potential consequences of an option
- Engage in an exploratory mindset (*correct response*)
- Explain each other's perspective to a third party
- Use a key assumptions check

**Feedback:** *An exploratory mindset focuses on collaborative problem solving.*

Question 3 of 4. Which technique would you use to resolve the relative importance assigned to pieces of information?

- Brainstorm potential consequences of an option
- Engage in an exploratory mindset
- Explain each other's perspective to a third party
- Use a key assumptions check (*correct response*)

**Feedback:** *A key assumptions check can be helpful in weighting the value of information for analysis.*

Question 4 of 4. Which technique would you use to clear a misunderstanding between two team members?

- Brainstorm potential consequences of an option
- Engage in an exploratory mindset
- Explain each other's perspective to a third party (*correct response*)
- Use a key assumptions check

**Feedback:** *The mutual understanding approach requires each side to understand the other person's perspective well enough to explain it to someone else.*