Preserving Investigative and Operational Viability in Insider Threat

Student Guide

September 2017

Center for Development of Security Excellence

Lesson 1: Course Introduction

Overview

Welcome

Your Insider Threat Program works diligently to detect, deter, and mitigate a wide range of threats posed by trusted insiders. Most incidents handled by your office will not result in the apprehension of a spy or even identify someone committing a crime. Remember that a main goal of the Program is to detect potential risk indicators and provide appropriate response actions. These actions guide individuals off of the critical pathway and mitigate risks before they manifest in espionage or other behaviors.

While most insider threat matters will be mitigated internally, some insider threat incidents will require reporting and referral actions that may result in counterintelligence or law enforcement investigations, inquiries, or operations, and/or legal proceedings. The actions of Insider Threat Programs can affect the outcome of these cases. It is essential for Insider Threat Programs to develop their internal policies, procedures, and authorities with the goal of ensuring that their actions do not impact these cases negatively.

But how do these cases get to court? And what happens when the incident and/or your agency garner the attention of the media? What must Insider Threat Programs consider when developing their protocols to ensure the Program does not interfere with law enforcement and counterintelligence actions, which could negatively impact future judicial proceedings?

Welcome to the *Preserving Investigative and Operational Viability in Insider Threat* course!

Objective

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

- Indicate the responsibilities of an Insider Threat Program in preserving investigative and operational viability when taking Insider Threat Program actions

Lesson 2: CI and LE Referrals

Introduction

Lesson Overview

Policies require Insider Threat Programs to detect, deter, and mitigate insider threats. In the course of your duties, your Program will gather, analyze, assess, respond to, and report insider threat matters. Your organization may refer to these collective activities as inquiries or investigations, and most matters will likely be resolved internally. However, in some cases the Program response will be to report or refer the matter elsewhere.

This lesson addresses:

- Reporting and referral by the Insider Threat Program to the appropriate counterintelligence (CI) and law enforcement (LE) agency
- The difference between your internal actions and the inquiries, investigations, or operations conducted by those entities
- The effect of your Program's actions on the success of those activities

Insider threat policies include:

- DoD: DoDD 5205.16, The DoD Insider Threat Program
- Federal Agency: Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
- Industry: National Industrial Security Program Operating Manual (NISPOM)

These policies are available from the Course Resources page.

Objectives

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

- State the purpose and requirements of reporting and referring insider threat matters
- Identify and define the actions that counterintelligence and law enforcement may take upon referral of insider threat matters

Reporting and Referral

Overview

When an Insider Threat Program identifies a potential insider threat or becomes aware of an insider threat matter, it has several response options, including mitigation, reporting, and referral. Insider Threat Programs can internally deploy actions designed to reduce the risk

associated with an individual. This occurs via elements organic to the organization—such as security, human resources, cybersecurity, and others—and in accordance with general counsel or other legal guidance. However, Insider Threat Programs are required to report certain types of information externally even as they explore internal mitigation options. In addition, Insider Threat Programs are required to refer some insider threat matters to CI or LE elements—either internal or external to the organization—for action.

To learn more about mitigation, refer to the *Insider Threat Mitigation Responses* course. You may register for this course through the Center for Development of Security Excellence (CDSE) website.

Term	Definition
Mitigate	Reduce the risk associated with an individual via a multidisciplinary response developed by internal subject matter experts in: • Security • Law enforcement • Counterintelligence • Mental health/behavioral science • Cybersecurity • Human resources • Legal
Report	Share information externally while continuing to pursue internal mitigation actions
Refer	Hand an insider threat matter over to counterintelligence or law enforcement for action

Purpose

Reporting and referral response options serve several purposes. First, they lay the foundation for deterring, detecting, mitigating, and, when appropriate, prosecuting insider threat activity, such as espionage, criminal activity, and security violations. They also help to establish patterns. For example, one security violation may not indicate an issue, but many violations over time may be an indicator. In addition, they aid in identifying geographically disparate, long-term, or other imprecise indicators, such as personnel issues associated with one individual across multiple employers. Finally, reporting and referral help your Insider Threat Program to maintain relationships and reciprocity with contacts within law enforcement, counterintelligence, and security that can help your Program fulfill its mission.

Requirements

Reporting regulations vary depending on whether you belong to the DoD, another federal agency, or cleared industry. All Insider Threat Programs have requirements to report specific information to the Federal Bureau of Investigation (FBI). In addition, DoD Insider Threat Programs are required to report threshold-level events to the DoD Insider Threat

Management and Analysis Center (DITMAC) and their cognizant DoD Law Enforcement Activity or Military Department Counterintelligence Office as appropriate. Industry Insider Threat Programs are also required to report to the Defense Counterintelligence and Security Agency (DCSA). In addition, Insider Threat Programs may need to report issues to local or federal law enforcement.

Laws, policies, and directives require Insider Threat Programs to refer some insider threat matters to CI and/or LE entities. These include:

- Threats and acts of violence
- Loss or compromise of classified information
- Physical or cyber breaches
- Foreign intelligence entity (FIE) activity
- Criminal activity

After referral, your Program may need to cease its activities. Coordinate with the entity and your General Counsel to determine the next steps after making a referral.

Refer to the *Insider Threat Mitigation Responses* course offered by CDSE for more information. You may register for this course through the CDSE website.

Reporting Entity	What to Report
FBI	• Unauthorized disclosure (DoD, Federal) • Foreign intelligence activity (DoD, Federal) • Actual, probable, or possible espionage, sabotage, terrorism, or subversive activities (Industry)
DITMAC	• Information meeting DITMAC reporting thresholds; contact the DITMAC for current thresholds (DoD)
Cognizant DoD Law Enforcement Activity or Military Department Counterintelligence Office	• Contacts, activities, indicators, and behaviors associated with foreign intelligence, international terrorism, and foreign intelligence entity associated cyberspace (DoD)
DCSA	• Actual, probable, or possible espionage, sabotage, terrorism, or subversive activities (Industry) • Adverse information (Industry)

CI and LE Actions

Overview

CI and LE complement the Insider Threat Program when mitigating the risks associated with an insider threat. CI and LE personnel may serve on your Insider Threat Hub or as part of

your insider threat team, along with security, cybersecurity, human resources, mental health and behavioral science, and legal personnel. The actions and authorities under which each discipline operates are distinct from each other.

Coordinate with your legal counsel to ensure that Insider Threat Program activities do not compromise a potential investigation or prosecution and that all activities are in accordance with privacy and civil liberties requirements.

Refer to the *Insider Threat Mitigation Responses* and *Developing a Multidisciplinary Insider Threat Capability* courses for more information. You may register for these courses through the CDSE website.

Reasonable Belief and Probable Cause

When an Insider Threat Program reports or refers a matter to CI or LE, that element must establish reasonable belief and/or probable cause to take certain actions. Note that the information your Program provides does not need to establish reasonable belief or probable cause, but will be used by CI and LE to pursue it. Once reasonable belief is established, CI or LE may conduct inquiries, investigations, or operations. Probable cause is the standard to conduct search and seizure, and military apprehensions or arrest.

Reasonable Belief

Reasonable belief means that the facts and circumstances are such that a reasonable person would hold the belief. The facts and circumstances must be articulable or capable of being expressed, explained, or justified. The basis for belief may be based on experience, training, and knowledge. Hunches and intuition are not sufficient.

Probable Cause

Probable cause means that reasonable grounds exist to believe that a specific individual has committed, is committing, or is about to commit an offense. Reasonable belief and the ability to articulate the facts and circumstances surrounding the matter form the basis of probable cause. Probable cause is the necessary level of belief to allow police seizures or arrests of individuals and full searches of dwellings, vehicles, and possessions.

Inquiry

CI and LE may conduct inquiries as proscribed by law or policy. Note that these are distinct from the inquiries or other activities conducted by the Insider Threat Program. An inquiry is the initial fact-finding and analysis process used to determine the facts of an incident. This allows CI and LE to determine whether further action is required and to establish jurisdiction. Specifically, DoD CI elements may conduct a CI inquiry to establish or refute a reasonable belief that a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in harmful activities.

Harmful activities may include:

- Espionage
- Treason
- Sedition
- Subversion
- Assassinations
- International terrorist activities

Note that other types of inquiries also exist. Your Insider Threat Program may undertake similar actions as an administrative inquiry, for example. The DoD also recognizes other types of inquiries. These are subject to DoD policy and distinct from inquiry or response actions taken by Insider Threat Program offices. These include security inquiries undertaken by security personnel and counterintelligence insider threat inquiries undertaken by authorized CI personnel.

Investigation

An official investigation is a systematic inquiry into an allegation of unfamiliar or questionable activities. Investigations are initiated when there are articulable facts that indicate a violation of law or policy. Investigations gather evidence to substantiate or refute the allegation using CI and LE authorities and methodologies.

Evidence: Information or objects that may be admitted into court for judges and juries to consider when hearing a case (e.g., testimony, physical items, fingerprints)

Operation

A counterintelligence operation is the process by which CI or LE elements systematically collect and evaluate information. Counterintelligence operations are carried out to discover the capabilities and intentions of adversaries. Operations are conducted for military, strategic, DoD, or national security purposes against a target having suspected or known affiliation with FIEs, individuals with suspected involvement in criminal activity, and other foreign persons or organizations. Operations are also conducted to counter terrorism, espionage, or other illicit activities that threaten the security of the United States.

Review Activities

Review Activity 1

Which of the following may require referral to law enforcement or counterintelligence for investigation and possible prosecution?

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

- ○ Unusual work hours
- ○ Financial problems
- ○ Criminal activity
- ○ Alcohol abuse

Review Activity 2

Select the term that matches each definition. Then check your answers in the Answer Key at the end of this Student Guide.

Definition 1 of 5. Knowledge of such facts as would lead a reasonable person to believe that a particular individual is committing, has committed, or is about to commit an offense.

- ○ Inquiry
- ○ Investigation
- ○ Operation
- ○ Probable cause
- ○ Reasonable belief

Definition 2 of 5. The initial fact-finding and analysis process used to determine the facts.

- ○ Inquiry
- ○ Investigation
- ○ Operation
- ○ Probable cause
- ○ Reasonable belief

Definition 3 of 5. Systematic inquiry into an allegation.

- ○ Inquiry
- ○ Investigation
- ○ Operation
- ○ Probable cause
- ○ Reasonable belief

Definition 4 of 5. The facts and circumstances are such that a reasonable person would hold the belief.

- ○ Inquiry
- ○ Investigation
- ○ Operation
- ○ Probable cause
- ○ Reasonable belief

Definition 5 of 5. Intelligence and counterintelligence tasks performed for the purpose of discovering the capabilities and intentions of adversaries.

- ○ Inquiry
- ○ Investigation
- ○ Operation
- ○ Probable cause
- ○ Reasonable belief

Lesson 3: Considerations for Insider Threat Programs

Introduction

Lesson Overview

Your Insider Threat Program's actions prior to a referral to counterintelligence or law enforcement can affect the outcome of investigations, counterintelligence operations, and legal proceedings associated with the matter. In some instances, insider threat matters may also be the subject of media coverage.

This lesson addresses considerations for Insider Threat Programs to preserve investigative and operational viability.

Objectives

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

- Describe the consequences of improperly handling insider threat response actions, referrals, or information
- Explain the principles behind the proper handling of unclassified and classified evidentiary material

Program Authorities

Overview

Insider Threat Programs must develop internal procedures and processes for conducting mitigation response, administrative actions, or other Insider Threat Program functions. These procedures must be in accordance with all applicable regulations, policies, and directives. Work with your General Counsel to determine which legal authorities and policies apply to your organization.

In addition, Insider Threat Programs should develop a communications plan. The plan should describe the protocol for discussing insider threat matters with the media and other external elements. Coordinate with your organization's public affairs office and legal counsel when developing a communications plan. Before discussing an insider threat matter with the media or another external element, follow the guidance provided by the communications plan and your public affairs office.

Impacts

The Insider Threat Program's procedures, processes, and media communications may have far-reaching impacts on potential operations or investigations, individuals, and the effectiveness of the Insider Threat Program.

Inappropriate processes, actions, or media communications may lead to compromised or ineffective operations or investigations. This may also limit the ability to prosecute or pursue other judicial options.

For individuals, possible consequences include the violation of the individual's privacy or civil liberties and negative impacts on the individual's career and livelihood.

Finally, poor or poorly executed processes and media communications can impact the Program itself. These can affect the morale of personnel in a way that results in reduced vigilance and reporting. It may also increase the organization's vulnerability to lawsuits or other complaints.

Ultimately, these situations increase the risk of insider threat.

Considerations

Insider Threat Program standard operating procedures should include considerations for not alerting potential insider threats, reporting and referral timelines, and evidence handling and seizure.

Non-Alerting Protocol

While your Program may conduct its own initial activities to assess a situation, if you believe that the matter meets the threshold for reporting or referral, you should take steps to avoid alerting the subject of a potential inquiry, investigation, or operation. If the potential subject is alerted, it may compromise the activity, result in the destruction of evidence, or raise the potential for flight from prosecution.

In your Insider Threat Program's protocols, determine when you will limit or prohibit interviews of subjects and checks of certain data sets that have alert capabilities. For example, individuals that use credit monitoring services receive an alert when someone checks their credit. Also consider incorporating an internal limited distribution process. This limits the number of Program personnel with knowledge of the most sensitive matters.

Reporting and Referral Timelines

Incorporate timelines for reporting and referral. Delayed reporting or referral may increase your organization's insider threat risk. For example, the DITMAC sets reporting thresholds for DoD Insider Threat Programs. Delayed reporting or failure to report weakens the ability of the DITMAC to integrate data from multiple sources. This places

both the Component and the DoD at added risk. Delayed reporting or referral may also negatively impact investigations, inquiries, or operations carried out by CI or LE. Finally, if a significant amount of time has lapsed since the suspected activity, it may impede the ability to secure U.S. Federal Intelligence Surveillance Act (FISA) warrants; other court warrants; National Security Letters (NSLs); or preservation letters.

Work with your General Counsel to determine the best course of action during each referral process. Each matter is different. Your Insider Threat Program may be able to share information and continue to pursue mitigation options, in some instances.

To learn more about the DITMAC, refer to the DITMAC Short on the CDSE website.

Evidence Handling and Seizure

While Insider Threat Programs do not conduct investigations or operations, your Program's standard operating procedures should include provisions for incidental evidence handling and seizure. For example, there may be rare instances when the Program must take possession of and/or transmit physical or digital evidence associated with a potential insider threat.

When planning for these, coordinate with your Inspector General and/or General Counsel.

Evidence Handling

Overview

While Insider Threat Program authorities do not allow workplace searches, it is possible that information relevant to a future inquiry or investigation may be developed during the course of your actions. Any evidence your Insider Threat Program uncovers has the potential to play a critical role in the overall investigation and resolution of a suspected criminal act. Therefore, it is essential that the Program ensures that any evidence is acquired legally and handled properly so that it remains viable in case of future prosecution. In addition, the Program must also protect the civil liberties and privacy of employees.

Law of Evidence

Evidence laws govern the use of testimony and exhibits or other documentary material that is admissible in a judicial or other administrative proceeding. You do not need to be an expert in evidence handling, but you should coordinate with both your General Counsel and the agency receiving the referral when gathering or preserving information.

Your Insider Threat Program should also consider the effects and handling of the fruit of the poisonous tree doctrine, chain of custody, testimonial evidence, and exculpatory information.

Fruit of the Poisonous Tree Doctrine

The fruit of the poisonous tree doctrine is a legal principle that excludes from introduction at trial any evidence later developed as a result of an illegal search or seizure.

It is essential that any information gathered by the Insider Threat Program—and any evidence subsequently developed from that information in an investigation or inquiry—is admissible in legal or administrative proceedings. Therefore, Insider Threat Programs must be sure to acquire evidence legally and handle it properly and to protect the privacy and civil liberties of employees.

For example, Insider Threat Program protocols may include placing banners on information systems that adequately disclose monitoring and routine use of information systems. Protocols may also include not conducting unauthorized searches of employees' virtual or physical workspaces.

Chain of Custody

"Chain of custody" refers to a chronological written record that reflects the release and receipt of evidence from initial acquisition until final disposition.

Insider Threat Programs must demonstrate the chain of custody for evidence gathered and shared so that a record exists that the evidence was acquired or received, processed or transferred, safeguarded, and disposed of properly.

For example, Insider Threat Program protocols may include using evidence identifiers such as tape, labels, containers, and string ties to identify the evidence, the person who collected the evidence, the date the evidence was gathered, basic information such as where it was gathered, and a brief description of the evidence.

Testimonial Evidence

Testimonial evidence is also subject to laws and regulations.

Insider Threat Programs must honor the Garrity rights of employees, which protect public employees from being compelled to incriminate themselves during investigatory interviews conducted by their employers. Garrity rights originate from the 1967 U.S. Supreme Court decision in Garrity v. New Jersey and stem from the Fifth Amendment to the U.S. Constitution, which declares that the government cannot compel a person to be a witness against him- or herself. Insider Threat Programs must also acknowledge the First Amendment, which guarantees individuals' right to free speech.

For example, Insider Threat Program protocols may include acknowledging that employees have the right to refuse to answer questions if it is related to potentially criminal conduct. Program protocols may also include training all insider threat personnel to recognize protected communications and speech.

Protected Communications and Speech: Certain communications, whether oral or electronic, may be protected and could include those subject to attorney-client privilege or other instances where there is a reasonable expectation of privacy. Work with your legal counsel to determine what types of speech and communication are protected and for proper guidance on the handling of such materials.

Exculpatory Information

Exculpatory information is evidence favorable to the defendant in a criminal trial that exonerates or tends to exonerate the defendant of guilt. This type of evidence tends to clear someone of fault or guilt.

Note that Insider Threat Programs are required to include any exculpatory information, if it exists, when making a report or referral.

Exonerate: Absolve from blame for a fault or wrongdoing, especially after due consideration of the case

Classified Information

Some information, evidence, or other parts of a referral may be classified.

Insider Threat Programs must ensure that classified information is protected in the process of reporting or referring. This includes adhering to the rules of marking classified information and transmitting the information via appropriate channels. DCSA and the FBI offer secure transmission options. For DoD Insider Threat Programs, the DITMAC also offers secure transmission options. Contact the referral entity to discuss the requirements, ensuring that initial requests for information are unclassified until you establish a secure means of communication.

Once the referral entity accepts the information, they also accept responsibility for further disclosure and abide by the Classified Information Procedures Act (CIPA).

Note that sensitive unclassified information may also require special handling considerations.

Classified Information Procedures Act (CIPA): The regulation which ensures the proper protection of classified information in indicted cases

Sensitive Information

Even unclassified information may sometimes be deemed too sensitive for normal reporting by a DoD Law Enforcement Activity or a Military Department Counterintelligence Organization. In those cases, the DITMAC has established a limited distribution reporting procedure in its case management system, known as the DITMAC System of Systems (DSoS).

Review Activities

Review Activity 1

Which of the following are possible consequences of improperly handling insider threat response actions?

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

- ☐ Compromised operations or investigations
- ☐ Inability to prosecute
- ☐ Violation of privacy or civil liberties
- ☐ Reduced vigilance and reporting

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 of the following is a written record that demonstrates the release and receipt of evidence?

- ○ Fruit of the poisonous tree doctrine
- ○ Chain of custody
- ○ Testimonial evidence
- ○ Exculpatory information

Question 2 of 4. Which of the following is the legal principle that excludes evidence developed as a result of an illegal search?

- ○ Fruit of the poisonous tree doctrine
- ○ Chain of custody
- ○ Testimonial evidence
- ○ Exculpatory information

Question 3 of 4. Which of the following refers to information that may exonerate the defendant of wrongdoing?

- ○ Fruit of the poisonous tree doctrine
- ○ Chain of custody
- ○ Testimonial evidence
- ○ Exculpatory information

Question 4 of 4. Which of the following is subject to Garrity rights?

- ○ Fruit of the poisonous tree doctrine
- ○ Chain of custody
- ○ Testimonial evidence
- ○ Exculpatory information

Lesson 4: Course Conclusion

Course Summary

Summary

With their actions, Insider Threat Programs can affect the outcomes of high-profile insider threat matters, the ability of counterintelligence and law enforcement to take action, and the prosecution of insider threat cases. It is therefore essential that Insider Threat Programs carefully develop the internal policies, procedures, and authorities that govern their actions to avoid negatively impacting insider threat cases and their disposition.

Lesson Summary

Congratulations! You have completed the *Preserving Investigative and Operational Viability in Insider Threat* course.

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

- Indicate the responsibilities of an Insider Threat Program in preserving investigative and operational viability when taking Insider Threat Program actions

To receive course credit, you must take the *Preserving Investigative and Operational Viability in Insider Threat* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam. Otherwise, select the Take Exam button on the last screen of the course to take the online exam and receive your certificate.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

Which of the following may require referral to law enforcement or counterintelligence for investigation and possible prosecution?

- ○ Unusual work hours
- ○ Financial problems
- ⦿ Criminal activity *(correct response)*
- ○ Alcohol abuse

Feedback: *While unusual work hours, financial problems, and alcohol abuse may present a concern to be addressed by the Insider Threat Program, criminal activity must be referred to counterintelligence or law enforcement.*

Review Activity 2

Definition 1 of 5. Knowledge of such facts as would lead a reasonable person to believe that a particular individual is committing, has committed, or is about to commit an offense.

- ○ Inquiry
- ○ Investigation
- ○ Operation
- ⦿ Probable cause *(correct response)*
- ○ Reasonable belief

Feedback: *Probable cause means that facts would lead a reasonable person to believe that a particular individual is committing, has committed, or is about to commit an offense. Reasonable belief forms the basis for probable cause.*

Definition 2 of 5. The initial fact-finding and analysis process used to determine the facts.

- ⦿ Inquiry *(correct response)*
- ○ Investigation
- ○ Operation
- ○ Probable cause
- ○ Reasonable belief

Feedback: *An inquiry is the initial fact-finding and analysis process used to determine the facts of an incident.*

Definition 3 of 5. Systematic inquiry into an allegation.

- ○ Inquiry
- ⦿ Investigation *(correct response)*
- ○ Operation
- ○ Probable cause
- ○ Reasonable belief

Feedback: *An investigation is a systematic inquiry into an allegation of unfamiliar or questionable activities.*

Definition 4 of 5. The facts and circumstances are such that a reasonable person would hold the belief.

- ○ Inquiry
- ○ Investigation
- ○ Operation
- ○ Probable cause
- ⦿ Reasonable belief *(correct response)*

Feedback: *Reasonable belief means that the facts and circumstances are such that a reasonable person would hold the belief.*

Definition 5 of 5. Intelligence and counterintelligence tasks performed for the purpose of discovering the capabilities and intentions of adversaries.

- ○ Inquiry
- ○ Investigation
- ⦿ Operation *(correct response)*
- ○ Probable cause
- ○ Reasonable belief

Feedback: *An operation refers to the intelligence and counterintelligence tasks carried out for the purpose of discovering the capabilities and intentions of adversaries.*

Lesson 3 Review Activities

Review Activity 1

Which of the following are possible consequences of improperly handling insider threat response actions?

- ☑ Compromised operations or investigations *(correct response)*
- ☑ Inability to prosecute *(correct response)*
- ☑ Violation of privacy or civil liberties *(correct response)*
- ☑ Reduced vigilance and reporting *(correct response)*

Feedback: *All of these are possible consequences of improperly handled insider threat response actions, referrals, information, or media communications.*

Review Activity 2

Question 1 of 4. Which of the following is a written record that demonstrates the release and receipt of evidence?

- ○ Fruit of the poisonous tree doctrine
- ⦿ Chain of custody *(correct response)*
- ○ Testimonial evidence
- ○ Exculpatory information

Feedback: *Chain of custody refers to a chronological written record that reflects the release and receipt of evidence from initial acquisition until final disposition.*

Question 2 of 4. Which of the following is the legal principle that excludes evidence developed as a result of an illegal search?

- ⦿ Fruit of the poisonous tree doctrine *(correct response)*
- ○ Chain of custody
- ○ Testimonial evidence
- ○ Exculpatory information

Feedback: *The fruit of the poisonous tree doctrine is a legal principle that excludes from introduction at trial any evidence later developed as a result of an illegal search or seizure.*

Question 3 of 4. Which of the following refers to information that may exonerate the defendant of wrongdoing?

- ○ Fruit of the poisonous tree doctrine
- ○ Chain of custody
- ○ Testimonial evidence
- ⦿ Exculpatory information *(correct response)*

Feedback: *Exculpatory information is evidence favorable to the defendant in a criminal trial that exonerates or tends to exonerate the defendant of guilt.*

Question 4 of 4. Which of the following is subject to Garrity rights?

- ○ Fruit of the poisonous tree doctrine
- ○ Chain of custody
- ⦿ Testimonial evidence *(correct response)*
- ○ Exculpatory information

Feedback: *Garrity rights protect public employees from being compelled to incriminate themselves in interviews with their employers.*