Student Guide
Privacy and Civil Liberties Overview

Course Introduction

Why are Privacy and Civil Liberties Important?

Screen 1 of 3

Narrator: The insider threat is not a new phenomenon. Since the dawn of our nation, insiders have used their access to cause harm through acts of espionage, sabotage, terror, unauthorized disclosure of classified information, and to commit acts of violence.

Narrator: In response to this threat, Federal and DoD policy established the requirement for Insider Threat programs to deter, detect, and mitigate actions by insiders that may pose a threat to national security.

Narrator: These policies authorize Insider Threat programs to gather and analyze information related to potential insider threats and to exercise response options to mitigate risk. However, with this authority comes great responsibility.

Narrator: All Insider Threat programs, including those undertaken by federal agencies, DoD components, and industry, are charged with the protection of individual privacy and civil liberties in the course of their actions. Efforts to mitigate insider threats must not compromise the rights of the workforce.

The implementation of institutional protections within an Insider Threat program that maintains security practices while protecting individuals' liberty and privacy interests is critical to mission success. Both of these goals are achievable and emphasis on one does not necessarily act to the detriment of the other. Failure to protect privacy and civil liberties can result in severe adverse impacts for individuals, undermine morale, and subject you and your organization to legal consequences.

Conversely, insider threat programs that follow law, policy, and regulations supporting privacy and civil liberties will enhance an organization’s ability to accomplish the mission and enable greater protection of national security.

Introduction

Screen 2 of 3

Image of the Constitution of the United States of America.

Narrator: Welcome to the Privacy and Civil Liberties Overview course.

Narrator: This course provides you with a high-level explanation of the importance that civil liberties, privacy laws, regulations, and policies have on conducting Insider Threat program actions.

Narrator: The course includes a scenario in within which you play the role of a new analyst assigned to the Insider Threat Hub team for an organization. This scenario will provide information and test your knowledge of protecting individuals' privacy and civil liberties while conducting insider threat tasks.

Course Objectives

Screen 2 of 3

A watermark image of the Constitution of the United States of America with the course objective listed as follows:

Course Objectives*:*

- Given instruction, the learner will be able to identify federal laws, policies, and regulations that ensure privacy and civil liberties.
- Given instruction, the learner will be able to explain why appropriate consideration of civil liberties and privacy is important for a successful Insider Threat program.
- Given instruction, the learner will be able to explain insider threat challenges impacted by socially charged matters regarding civil liberty laws and policies.
- Given instruction, the learner will be able to explain how to implement institutional protections within an Insider Threat program that maintain a proper balance between security practices and individuals' liberty and privacy interests.

Narrator: The Privacy and Civil Liberties Overview course includes four lessons and takes approximately 90 minutes to complete. Please review the course objectives listed on screen.

Privacy and Civil Liberties Guidelines Lesson

First Day

Screen 1 of 18

Rachel: Hi! I've been expecting you. Welcome to our Hub team. I'm Rachel, the Insider Threat Program Manager. Before we put you to work managing the insider risk, we need to get you up to speed on our responsibilities regarding privacy and civil liberties.

A popup appears on screen that lists the following lesson one objectives:

- Describe the societal importance of privacy and civil liberties.
- Identify the Constitutional protections, Privacy Act, and reasonable expectation of privacy in the workplace.

- Identify information that is protected as personally identifiable information (PII) and under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Rachel: Our goal is to ensure you are prepared to meet the daily challenges that you will face. We will start by identifying the federal laws, policies, and regulations that ensure privacy and civil liberties. These are our objectives while discussing the privacy and civil liberties guidelines. I'll let you get settled in your office first. Then, I'll give you a call and we can discuss the privacy and civil liberties information that you must be aware of when you monitor for insider threats and conduct incident response tasks.

Balancing National Security and Public Interest

Screen 2 of 18

A text box appears "You have settled into your office…". A text box appears "Select the phone to answer the call."

Balancing National Security and Public Interest

Screen 3 of 18

Rachel: Hello. Hope you are all settled in. Before we dive into the laws and policies, you need to understand that our privacy and civil liberties help maintain workforce and public trust in the U.S. Government. We must meet National security and public safety needs while preserving individual constitutional and legal protections afforded to all Americans.

Public trust in the Government is so critical that the 2004 9/11 Commission report recommended the creation of what is now the Privacy and Civil Liberties Oversight Board to consider the public's liberty concerns when reviewing the Government's actions to protect national security.

Also, Insider Threat Programs developed under Executive Order 13587 are mandated to ensure the responsible sharing and safeguarding of classified information in a manner consistent with applicable laws and appropriate protections for privacy and civil liberties.

In fact, all insider threat programs, whether in the federal government, DoD, or Industry, must protect privacy and civil liberties in the conduct of their duties.

I'm going to send you some more information about this. Look for an email coming your way soon. Bye.

The Insider Threat Program's Role

Screen 4 of 18

Audio plays "You've got mail." Highlight appears on a computer in image.

Hi,

Continuing from our phone conversation, we already discussed that public trust in the U.S. Government is essential, but you may be asking yourself how the Insider Threat Program fits in.

Insider Threat programs must consider privacy, civil right, and civil liberty concerns while implementing laws, regulations, and policies related to efforts to protect national security.

In other words, protecting the privacy and civil liberties of our workforce is one of our more significant responsibilities.

Resources you should become familiar with are The National Insider Threat Policy and Minimum Standards and the Privacy and Civil Liberties Oversight Board (PCLOB). PCLOB reports may offer you some insight into the types of recommendations they make to protect civil liberties in pending policy and law.

What is The Freedom of Information Act (FOIA)?

Screen 5 of 18

Rachel: Hey! Now that you understand why employee and public trust in the Government are critical, we can discuss how to maintain that trust. One of the safeguards put in place to enable oversight of government activity is the Freedom of Information Act, otherwise referred to as FOIA.

Since 1966, FOIA has provided the public the right to request access to records from any federal agency. It is the law that keeps citizens in the know about their government and is part of a program to improve transparency of government activities. Federal agencies are required to disclose any information requested under the FOIA unless it falls under one of nine exemptions that protect interests such as personal privacy, national security, and law enforcement.

For insider threat programs within the DoD and federal government, FOIA may apply to the records we create (including emails and notes), but you should know that FOIA requests and exemption rules can be complex. Organizations that have a FOIA office can consult with that resource. Otherwise, you can coordinate FOIA requests with the legal team and privacy officials.

The nine FOIA exemptions are listed here in this document. You can have a look at them now, but just so, you know, these will be available to you in your resources. You can download them and view them at your convenience.

The FOIA Exemptions Job-Aid is linked on screen.

FOIA Request

Screen 6 of 18

Rachel: Any individual can submit a FOIA request to an agency's FOIA Office. The request must be in writing and reasonably describe the records sought. As you can see, FOIA helps the U.S. Government maintain the public's trust. You can view more information on FOIA requests from the FOIA website. Another great resource on FOIA is the U.S. Office of Special Counsel.

FOIA.gov

U.S. Office of Special Counsel

Rachel: Recall that Insider Threat programs must safeguard the public's trust by ensuring individuals' privacy and civil liberties are not violated.

However, before we can start that process, we need to know what legal protections are afforded the individual through the U.S. Constitution, laws, policies, and regulations. Kendra is our Legal Counsel and can explain the legal protections. I will set up a meeting for you.

What are Civil Liberties?

Screen 7 of 18

Audio plays "You've got mail." Highlight appears on computer in image. Text box appears, "Select the computer to continue."

From: Rachel

Subject: Legal Protections

Good Afternoon,

I set up a meeting for you with our Legal Counsel, Kendra. You can meet her in the conference room once you finish reading this email.

In the meantime, I will try to lay the foundations for your meeting. First, civil liberties generally are fundamental rights and freedoms protected by the Constitution of the United States. They include freedom of speech and press, the right to bear arms, due process of law, peaceful assembly, and the right to petition the Government.

You can think of civil liberties as limitations of government power (i.e., negative rights) rather than granting an affirmative/positive right to citizens. For example, the First Amendment limits Congress' ability to control speech and expression with "Congress shall make no law." The First Amendment does not say, "the people have the right to free speech." Civil liberties are usually constitutional limits of government power. Contrast this to civil rights, which are typically affirmative obligations imposed on the government by both the Constitution (e.g., Thirteenth and Fourteenth Amendments) and defined by statute (e.g., Title VII of the Civil Rights Act of 1964)

to promote equality and equal protection under the law regardless of individual characteristics, such as race, gender, or religion.

Also, remember that the Ninth Amendment says that the Bill of Rights is not exclusive. You have fundamental rights that are not in the Constitution, such as a reasonable expectation of privacy. You can view the U.S. Constitution and the Bill of Rights under the "America's Founding Documents" tab in the National Archives website. Hope this helps.

Thanks, Rachel

Meeting with Kendra

Screen 8 of 18

Text box appears, “You are meeting with Kendra in the conference room.” “Continue” button appears.

U.S. Constitutional Protections

Screen 9 of 18

Kendra: Hi. I’m Kendra. I’m the attorney for our Insider Threat program. I work with our legal team that includes a representative from our office of general counsel and a privacy official.

Rachel asked me to talk with you about the legal protections related to insider threat operations. Rachel filled me in on what she has covered with you; so, let's talk about how the Constitution relates to our insider threat duties.

Kendra is highlighted in yellow.

U.S. Constitutional Protections, Cont.

Screen 10 of 18

Screen text: 1st Amendment

Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Kendra: We all know the first amendment and its provisions for the freedom of religion, speech, press, and peaceful assembly. However, Insider Threat programs need to ensure their processes and procedures protect the rights of individuals to hold personal beliefs and practice free speech.

We can't protect all speech and the levels of protection may depend on an individual's status. Such as, whether or not they are a public employee. Statements that may not be afforded First Amendment protection can include those that are:

Public employee statements that reflect solely matters of internal or personal interest; false and defamatory statements about the agency and/or agency employees; statements that unduly disrupt the office, undermine a supervisor's authority or destroy necessary close working relationships; and threats, insults, or language recognized as "fighting words."

4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Kendra: The 4th Amendment covers searches and seizures. It boils down to this. A search is constitutional if it does not violate a person's "reasonable" expectation of privacy. So what does reasonable mean here? This inquiry embraces two distinct questions: first, whether the individual's conduct reflects "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable." We will cover reasonable expectation of privacy later on, but be aware that Insider Threat programs must be mindful of what they can look at when obtaining data and conducting monitoring.

5th Amendment

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Kendra: We all have seen or heard of individuals pleading the fifth on TV. However, the 5th Amendment includes the provision "…nor shall be compelled in any criminal case to be a witness against himself…" So you cannot be compelled by the Government to incriminate yourself. Insider Threat Programs are not designed to conduct interviews of potential subjects of investigation. Based on the circumstances of a particular incident, the Insider Threat program will refer the matter to other operational elements such as law enforcement, security, or counterintelligence. However, Insider Threat program personnel need to be careful not to overstep the 5th Amendment when conducting activities or inquiries.

9th Amendment

The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Kendra: The 9th Amendment is saying that other rights may exist in addition to the ones explicitly mentioned in the Constitution. The Government cannot violate them even though the Constitution doesn't list them. It has been interpreted as justification for broadly reading the Bill of Rights to protect privacy in ways not specifically provided in the first eight amendments.

14th Amendment, Section 1

All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law that shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

Kendra: While the right to privacy is not explicitly spelled out in any one amendment, it has been determined by the Supreme Court to be inherent in several sections. However, the Due Process Clause of the 14th Amendment is cited most often. It ensures the states cannot make laws that violate citizens' rights, must follow due process, and ensures all citizens have equal protection under the law.

Now that we have the Constitution squared away let's move on to the Privacy Act of 1974.

Privacy Act of 1974

Screen 11 of 18

The following text is on the wall monitor:

The Privacy Act Policy

Privacy Act Policy Objectives

- To restrict disclosure of personally identifiable records maintained by agencies.
- To grant individuals increased rights of access to agency records maintained on them.
- To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
- To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Kendra: The purpose of the Privacy Act is to balance the Government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and

disclosure of personal information about them. The Privacy Act focuses on the four basic policy objectives listed here.

The Privacy Act applies to Federal agencies, including DoD, but not industry or state, local, tribal, or territorial governments. However, equivalent State laws may apply depending on location: The Privacy Act protects certain Federal Government records pertaining to individuals. In particular, the Act covers systems of records that an agency maintains and retrieves by an individual's name or other personal identifiers (e.g., social security number).

Kendra: As the slide states, the Privacy Act applies to federal agencies, including the Department of Defense, and individuals that have authorized access to their information systems, regardless of status. The Privacy Act does not apply to industry or state, local, tribal, or territorial governments. Those entities may be subject to other federal, state, and local privacy laws depending on their location and the nature of their organization. In general, the Privacy Act prohibits unauthorized disclosures of the records it protects. It also gives individuals the right to review records about themselves, to find out if these records have been disclosed, and to request corrections or amendments of these records, unless the records are legally exempt. It's important to note that Federal and DoD organizations will operate under a Systems of Records Notice or SORN that describes the nature of collection, retention, and dissemination of records. If an agency has a "record" that is not maintained in a "system of record," it generally may not be disclosed unless by consent.

Exceptions to the Consent Rule

1. To agency or organization employees with a legitimate need to know
2. For when the FOIA requires release
3. For a “routine use” identified in the System of Records Notice (SORN) that has been published in the Federal Register
4. To the Census Bureau for the purpose of conducting the census
5. For statistical research and reporting in which individuals will not be identified
6. To the National Archives and Records Administration
7. To civil or criminal law enforcement under U.S. control
8. For compelling circumstances affecting the health or safety of the individual
9. To either House of Congress
10. To the GAO
11. Pursuant to a court order (a subpoena signed by a judge)
12. To a consumer reporting agency in accordance with the Debt Collection Act

Kendra: The Consent Rule states that the individual subject of the file must provide consent to allow disclosure of information from a Privacy Act system to a third party; however, there are 12 exceptions to the consent rule. I listed the exceptions on the screen, but I have them all on this on a document for you to take with you. It also includes a link to the Department of Justice's Office of Information Protection Justice Information Sharing webpage.

The Privacy Act Consent Rule Exceptions Job-Aid is linked on the screen.

Case Law

Screen 12 of 18

Kendra: Some of our legal protections do not come directly from the Constitution nor laws passed by Congress or signed by the President. Case law has outlined some of our privacy and civil liberties. So let's talk about a few notable cases.

The following text appears on screen:

O'Connor v. Ortega, 480 U.S. 709 (1987) - Fourth Amendment protections apply to public employees under investigation for violations of employer policy, but only reasonable suspicion is necessary for a search to be conducted; courts must consider operational realities of public workplaces when violations of Fourth Amendment are alleged.

Kendra: The first case we need to discuss is O'Connor v. Ortega. To summarize, Dr. Ortega was terminated after his supervisors found allegedly incriminating evidence in his office while he was on administrative leave pending an investigation of alleged misconduct. The court held that individuals do not lose Fourth Amendment rights merely because they work for the government, instead of a private employer.

Having said that, while searches and seizures by government employers of the private property of employees are subject to 4th Amendment constraints, there are operational realities of the workplace that may make public employee's expectation unreasonable.

The court indicated this assessment of an individual's reasonable expectation of privacy is no different than a private employee – specifically, in the context of the employment relationship and cited the government's need for supervision, control, and efficient operation of the workplace.

The screen text changes to the following:

Garrity v. New Jersey 385 U.S. 493 (1967)

Police officers being investigated were given a choice either to incriminate themselves or to forfeit their jobs under New Jersey statute on The grounds of self-incrimination, and officers chose to make confessions, confessions were not voluntary but were coerced, and Fourteenth Amendment prohibited their use in subsequent criminal prosecution in state court. Garrity applies to all public employees.

Kendra: The next case involves the Fifth Amendment in regards to self-incrimination. Edward Garrity and five other police officers were suspected and subsequently interviewed in connection with "ticket fixing." During the interview, the officers' jobs were threatened if they did not cooperate with the investigation, which subsequently led to criminal charges. The court held that law enforcement officers and other public employees have the right to be free from compulsory self-incrimination. It gave birth to the Garrity warning, which is administered by investigators to suspects in internal and administrative investigations.

The screen text changes to the following:

Pickering v. Board of Education, 391 U.S. 563 (1968)

Pickering involved a Township High School teacher who was dismissed after writing a letter to a local newspaper, which criticized how the Township Board of Education and the district superintendent had handled past proposals to raise new revenue for the schools.

The Board of Education rejected the claim that the First and Fourteenth Amendments protected his writing of the letter. He appealed the Board's action to the Circuit Court of Will County and then to the Supreme Court of Illinois, which both affirmed his dismissal. The Supreme Court of the United States agreed the teacher's First Amendment right to free speech was violated and reversed the decision of the Illinois Supreme Court.

Kendra: Pickering versus the Board of Education is an excellent case to highlight the freedom of speech and the First Amendment. The court held that in the absence of proof of the teacher knowingly or recklessly making false statements the teacher had a right to speak on issues of public importance without being dismissed from his or her position.

Kendra: We could spend an entire day discussing case law that has helped shape our privacy and civil liberties. So I put together a list of cases that you can look over at your convenience. If you have legal questions in the future, don't hesitate to contact me. You should head back to your office; I'm sure Rachel would like to talk with you. Thanks for stopping by.

Privacy and Civil Liberties Case Law Examples is linked in the document.

Privacy Act of 1974

Screen 11 of 18

Text box appears. "After meeting with Kendra, you return to your office…"

Continue button appears.

Audio sound of telephone ring.

Reasonable Expectation of Privacy

Screen 13 of 18

Rachel: Hi, I was speaking to Kendra about the information she covered with you. It's all good stuff to keep in mind as you work with our Insider Threat team. As you learned from O'Connor v. Ortega, individuals do not lose Fourth Amendment rights just because they work for the government versus a private employer and Garrity rules will apply to public employees.

On the other hand, Insider Threat Program Requirements under EO 13587, the National Minimum Standards, DoD Directive 5205.16, the NISPOM, and ISL2016-02 require user

activity monitoring of classified systems. It is important to know that despite this requirement, there are still some expectations of privacy on government electronic devices. Therefore, Government employees have some expectation of privacy in the workplace.

For example, our computer system administrator cannot arbitrarily go searching for files with the primary purpose of obtaining evidence. Even with the banners we have on the computers, any action taken must be pursuant to authority given to that position and may be subject to attorney, medical, or chaplain privileges depending on the exact wording of the banner.

As a rule, Insider Threat programs do not conduct investigatory actions. However, even for a preliminary inquiry or other action taken by our office, the best course of action is to consult with our general counsel or legal insider threat hub member before gathering information to ensure that it is done legally.

Let's change our focus to some of the information that Insider Threat program personnel must protect during incident response activities. I am conducting a protected information briefing in the conference room with the rest of the Insider Threat team in a little bit. Why don't you join us and meet the rest of the team?

What is Personally Identifiable Information?

Screen 15 of 18

Text box appears. "You join the team in the conference room for the Protected Information briefing…"

Continue button appears.

Screen text displayed:

What is Protected Information?

Rachel: Hello everyone! Glad you could attend the protected information briefing. Before we get started, we have a newcomer joining the team. So let me introduce everyone. Starting on the right, you have met Kendra our Legal Counsel, next to her is Evan from Human Resources. Next is Layla our Behavioral Science Specialist; Connor is the team's Security Expert. On the other side of the table, we have Trinity, our Cybersecurity Specialist, Ethan from Counterintelligence and last but certainly not least is Aaron our Law Enforcement Expert. Each of these team members contributes to the conduct of the Insider Threat program and can ensure that we act in accordance with law and policy. Team this is our new Insider Threat analyst. Ok, let's get started with the briefing.

What is Protected Information?

As an Insider Threat program operator or manager, you may encounter Personally Identifiable Information (PII) and a subset known as Protected Health Information (PHI) in the course of an

incident response. You are responsible for protecting this information from unauthorized release. Failure to do so could result in criminal and civil penalties.

Rachel: So why do you need to know this and what are we talking about when we say protected information. As an Insider Threat program operator or manager, you may encounter PII and a subset known as PHI in the course of an incident response. You are responsible for protecting this information from unauthorized release. Failure to do so could result in criminal and civil penalties. But, we are not talking about classified information. We are talking about the need to protect personal information from unauthorized release to ensure we are protecting the privacy of our workforce.

What is PII?

The term Personally Identifiable Information refers to information used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Rachel: PII is information that we can use to distinguish or trace an individual's identity, alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information used to distinguish or trace an individual's identity, the term PII is necessarily broad.

What is protected as PII?

The PII the government collects must be relevant, accurate, timely, and complete. PII can be used to distinguish or trace an individual's identity, such as:

- Name
- Social Security number
- Biometric record or identifier
- Work ID numbers

Rachel: We all have personal information that we use to identify ourselves. This information could be a driver's license number, an address, a birthdate, or even a previous health condition. The Federal Government collects and maintains PII about individuals in order to govern; for example, to track Social Security payments, collect taxes, and guarantee citizens' right to vote. Now let’s talk about PHI and the types of information covered by the Health Insurance Portability and Accountability Act of 1996, also known as HIPAA.

The HIPAA Privacy Rule

Screen 16 of 18

Screen text displayed:

What is HIPAA Privacy Rule?

Rachel: First let's discuss HIPAA, specifically, the HIPAA Privacy rule.

The screen text changes to the following:

The HIPAA Privacy Rule Standards

This rule addresses the use and disclosure of individuals' health information, called "protected health information" by organizations subject to the Privacy Rule, referred to as "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.

Rachel: Rachel: A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and wellbeing. Given that the health care marketplace is diverse, the rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures.

The screen text changes to the following:

What is PHI?

Individually identifiable health information that a covered entity creates or receives, relating to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Rachel: Now let's discuss PHI. Not all PHI is governed by HIPAA but, as a subset of PII, it carries all of the basic safeguarding requirements that apply to PII, with additional safeguards. So, like PII, we need to protect PHI from unauthorized release. Failing to do so could subject us to criminal and civil penalties.

The screen text changes to the following:

Would you like to know more about PII? Identifying and Safeguarding Personally Identifiable Information (PII) DS-IF101.06

Rachel: That's all I have for you on the protected information. If you would like to explore PII and PHI further, I suggest taking DS-IF101.06, the Identifying and Safeguarding PII course offered by CDSE. I'd like our new analyst to meet me in my office. Thanks everyone for coming.

Scenario Knowledge Check 1

Screen 17 of 18

Rachel: It's been a busy day for you! We discussed the importance of privacy and civil liberties, as well as the legal responsibilities to safeguard them.

You also just attended the briefing covering protected information. So let me ask you a question.

This situation happened just a few months ago. During a review of an organization's on-boarding processes, the management asked the Insider Threat team to review employment forms for any information considered PII. What types of information should the team look for?

Pop up screen text displayed:

During a review of an organization's on-boarding processes, the Insider Threat team was asked to review the employment forms for any items that would be considered Personally Identifiable Information.

Of the items listed, which should the team highlight as PII? Select all that apply.

A. **Social Security Number**
B. **Address**
C. **Name**
D. **Position Description**

End of First Day

Screen 18 of 18

Rachel: I have to say I am impressed. We piled a ton information on you, and you seem to be absorbing it very quickly.
We talked about the societal importance of privacy and civil liberties, then we covered some of the legal protections we all have, and finally we discussed protected information we are responsible for safeguarding. Let's stop for today. We can start up again tomorrow by discussing why appropriate consideration of civil liberties and privacy is important for Insider Threat programs.

Civil Liberties, and Insider Threat Programs Lesson

The Following Morning

Screen 1 of 10

Rachel: Good Morning! It's good to see you. Well we have another busy day planed for you. Today we will be discussing why appropriate consideration of privacy and civil liberties is important for successful Insider Threat programs.

A popup appears on screen that lists the following lesson one objectives:

Lesson 2 Objectives

- Describe common civil liberties and privacy complaints including the legal consequences for violating an individual's privacy and civil liberties.
- Describe how Operations Security can be employed to safeguard information including PII, PHI, and information subject to HIPAA.
- Explain how the principle of confidentiality applies to insider threat activities.

Rachel: To get you to that level of understanding, you will have to meet the objectives you see here. We will meet in the conference room in a little while. Why don't you go to your office for now? I sent you an email with some information to review before the meeting.

Common Types of Complaints

Screen 2 of 10

Audio, "You have new Email."

Image of computer is highlighted in yellow.

Email Text:

From: Rachel

Subject: Common Civil Liberties and Privacy Complaints

Good Morning Team,

This morning we are going to meet in the conference room to talk about some common privacy and civil liberties complaints. Some may ask what types of civil liberties complaints we receive most frequently. Well, in the DoD, complaints alleging violations of the First, Fourth, and Fifth Amendments to the Constitution seem to top the list. Other agencies and organizations note the receipt of frequent complaints about the breach of personally identifiable information. Here is a list of the common issues I would like you to review prior to our meeting.

- Unauthorized Release or Breach of PII data
- First Amendment complaints involving:
  - Freedom of speech, religion, or the press
  - Right to peaceably assemble or petition the government
  - Fourth Amendment complaints may include claims of unreasonable searches/seizures.
  - Fifth Amendment complaints may include issues involving:
    - Deprivation of life, liberty, or property without due process
    - Double jeopardy (being punished twice for the same crime)
    - Self-incrimination

See you all soon.

VR,

Rachel

Common Civil Liberties and Privacy Complaints

Screen 3 of 10

Text box appears, "You join the team in the conference room to discuss Common Civil Liberties and Privacy Complaints."

Screen text displays the following:

Common Civil Liberties and Privacy Complaints

Rachel: Hello everyone! I hope you all had a chance to read my email. As you already know, we are going to discuss some common civil liberties and privacy complaints. So, I would like to do this a little different then our standard meeting. I would like to explain some complaint scenarios, and I would like you, our new analyst to tell us which Constitutional Amendment was possibly violated. Ok, let's get started.

Rachel: Our first situation involves an individual that complained that they were unfairly monitored by the Insider Threat program because of their religious background. So which Amendment addresses this complaint?

Screen text displays the following:

Complaint 1 - A complainant alleged that they were unfairly monitored by the Insider Threat program because of their religious background. Which Amendment addresses this complaint?

A. The First Amendment
B. The Second Amendment
C. The Fifth Amendment

Common Complaints (First)

Screen text displays the following:
Complaint 1 - A complainant alleged that they were unfairly monitored by the Insider Threat program because of their religious background. Which Amendment addresses this complaint? l

The First Amendment

Kendra: The Insider Threat program's actions may be in violation of the First Amendment if an individual was monitored by the program based on a protected status, such as religious beliefs, rather than based on conduct or behavior then.

Common Complaints (Second)

Screen text displays the following:

Complaint 1 - A complainant alleged that they were unfairly monitored by the Insider Threat program because of their religious background. Which Amendment addresses this complaint?

The Second Amendment

Feedback: The First Amendment may involve the following issues:

- Freedom of speech, religion, or the press
- Right to peaceably assemble or petition the government

Common Complaints (Fifth)

Screen text displays the following:

Complaint 1 - A complainant alleged that they were unfairly monitored by the Insider Threat program because of their religious background. Which Amendment addresses this complaint?

The Fifth Amendment

Aaron: Well, the Fifth Amendment states: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation." I would think that applying the Fifth Amendment to this complaint would be ineffective. I don't see any mention of a lack of due process, being punished twice for the same crime, or self-incrimination in this complaint.

Arron highlighted in yellow on screen.

Screen text displays the following:

Complaint 1 - A complainant alleged that they were unfairly monitored by the Insider Threat program because of their religious background. Which Amendment addresses this complaint?

The Fifth Amendment

First Amendment may involve the following issues:

- Freedom of speech, religion, or the press
- Right to peaceably assemble or petition the government

Legal Consequences for Violations

Screen 4 of 10

Screen text displays the following:

Legal Consequences for Violations

The Government and individual employees may be subject to both Civil and Criminal penalties for violating the Privacy Act.

Rachel: We cannot unfairly target individuals or tarnish their reputations by unnecessarily exposing that they were the subject of an unsubstantiated insider threat inquiry.

Also, consider that there may be legal repercussions for violating applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information.

In other words, we as an organization and as individuals can face civil or criminal actions for violations. So be mindful of the actions you take while handling information and conducting insider threat duties. Thanks everyone for taking the time for this.

Use of Operations Security (OPSEC) to Safeguarding Information

Screen 5 of 10

Audio, "You have new Email."

Image of computer is highlighted in yellow.

Email Text:

From: Rachel

Subject: Use of Operations Security (OPSEC) to Safeguarding Information

Hello,

I wanted to email you as soon as we finished briefing in the conference room. I did not want you to think that we are operating without protection or procedures for protecting privacy and civil liberties. EO 13587 required structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that are consistent with appropriate protections for privacy and civil liberties.

To achieve this we use the OPSEC process to prevent the inadvertent compromise of sensitive or classified information. OPSEC was not designed specifically for the Insider Threat program, but its process works well for our purposes.

I have some training on the OPSEC process that I want you to review. Select the link below to start the training.

OPSEC Process

VR,

Rachel

The OPSEC Process

Screen 6 of 10

Screen text displays the following:

The OPSEC Five-Step Process

Select each step of the process in the graphic to learn more.

Identification of Critical Information

Critical information is factual data about an organization's intentions, capabilities, and activities that the adversary needs to plan and act effectively to degrade operational effectiveness or place the potential for organizational success at risk. The OPSEC process identifies critical information and determines when that information may cease to be critical in the life cycle of an operation, program, or activity.

What information must be protected? PII including PHI, HIPAA information, and other controlled unclassified information.

Why does this information need to be protected? To safeguard privacy and civil liberties and to protect mission effectiveness.

Analysis of Threats

Threat analysis consists of determining the adversary's ability to collect, process, analyze, and use information.

Who might want the information? Identify thieves and adversaries looking to target and/or recruit employees.

What are their intentions and what are they capable of doing to get the information? This is dependent on the adversaries, but there have been plenty of recent examples of both careless actions and malicious data breaches resulting in the loss of employee information.

Assessment of Risks

Risk assessment is the heart of the OPSEC process. In a risk assessment, threats and vulnerabilities are compared to determine the potential risk posed by an adversary. When the level of vulnerability is assessed to be high and the adversary threat is evident, then adversary

exploitation is expected, and risks are assessed to be high. When the vulnerability is slight, and the adversary's collection ability is rated to be moderate or low, the risk may be determined to be low, and less extensive protective measures may be required.

If someone gets the information, how will that affect the mission? In the case of insider threat, improper handling of PII or other sensitive material may make people less willing to come forward with reporting if they think the Insider Threat program will be careless with the information.

How will that impact the individual whose information was lost? Among other things, the individual could be subject to identity theft, public embarrassment, or even targeting by a foreign intelligence entity.

What will be the overall impact of the loss of the critical information?

- Individuals may be harmed
- People will lose faith in the Insider Threat program
- The program could be sued

Application of Appropriate Countermeasures

In the final step of the OPSEC process, countermeasures are developed to protect the activity. Ideally, the chosen countermeasures eliminate the adversary threat, the vulnerabilities that can be exploited by the adversary, or the utility of the information.

This step sums up the OPSEC process by answering this question: What will be done to protect critical information?

When the last graphic is select, an EXIT button appears.

What is the Principle of Confidentiality?

Screen 7 of 10

From: Rachel

Subject: The Principle of Confidentiality

Attachment: Principle of Confidentiality.pdf

Good Afternoon Team,

I wanted to pull together some of the things we have been discussing today. We've looked at the common complaints related to privacy and civil liberties, the consequences of failing to address these issues, and the OPSEC process we use to protect information. It is clear that appropriate consideration of civil liberties and privacy is necessary for a successful Insider Threat program.

These considerations are summed up by the Principle of Confidentiality, which discusses:

- Fair information practices
- Limitations on information sharing
- Preventing negligent damage to an individual's reputation
- Information use restrictions

Select the attachment to review the main points of the Principle of Confidentiality. I would like to meet in the conference room in a few minutes so we can wrap up the day.

VR, Rachel

The Principle of Confidentiality document is linked on screen.

Scenario Knowledge Check 1

Screen 8 of 10

Rachel: Good to see you all again. I called you all in to do a quick review of our discussions today. We discussed why appropriate consideration of privacy and civil liberties is important for a successful Insider Threat program. We talked about common civil liberties and privacy complaints and consequences for violations. We also discussed the OPSEC process and the principle of confidentiality. Our new analyst is really sharp and is going to be a great asset to the program. Go ahead and ask some questions. You'll see how much was learned these last few days.

Layla: Hey Rachel, I have one. An Insider Threat analyst reviewed our email policy and procedure to identify faults or weaknesses that could be exploited by insider threats. Which step of the OPSEC process would the analyst apply in this situation?

Pop up screen text displayed:

An Insider Threat program from another organization discovered that security personnel were conducting random searches of the An Insider Threat analyst reviewed our email policy and procedure to identify faults or weaknesses that could be exploited by insider threats. Which step of the OPSEC process would the analyst apply in this situation?

A. Analysis of vulnerabilities
B. Analysis of threats
C. Assessment of risks
D. Application of appropriate countermeasures

Scenario Knowledge Check 2

Screen 9 of 10

Rachel: That was a good one Layla! Good job. Let's try one more. Aaron do you have a question for our new analyst?

Aaron: All right, this one is a hard one, so I hope you paid attention. A member of an Insider Threat team mistakenly placed multiple files that contained derogatory Protected Health Information (PHI) on an unsecured server. The information remained on the server for over a week, and accessed several times before it was noticed. Several weeks later, two individuals who were the subjects of the PHI filed complaints with their Equal Employment Opportunity office claiming they were not selected for a project due to rumors based on the unauthorized release of their PHI. So, which part of the principle of confidentiality was not taken into consideration in this situation?

Pop up screen text displayed:

A member of an Insider Threat team mistakenly placed multiple files that contained derogatory Protected Health Information (PHI) on an unsecured server. The information remained on the server for over a week, and accessed several times before it was noticed. Several weeks later, two individuals who were the subjects of the PHI filed complaints with their Equal Employment Opportunity office claiming they were not selected for a project due to rumors based on the unauthorized release of their PHI. Which part of the principle of confidentiality was not taken into consideration in this situation?

A. Preventing negligent damaging of an individual's reputation
B. The Privacy Act of 1974
C. Cybersecurity and information sharing
D. Treating the workforce with fairness

End of the Day Two

Screen 10 of 10

Rachel: Wow, excellent questions team! I think we are quickly getting our new analyst ready for conducting day-to-day program operations.

We talked about civil liberties and privacy complaints, to include consequences for violations. We also discussed the use of OPSEC for safeguarding information and the principle of confidentiality.

Let’s call it quits for today. Tomorrow our new analyst will dive into the Insider Threat Program challenges impacted by socially charged matters regarding civil liberty laws and policies. Have a good evening everybody.

Insider Threat Challenges with Privacy and Civil Liberties Lesson

The Morning; Day 3

Screen 1 of 12

Rachel: Good Morning! Well, we have another busy day planned for you. Today we will be discussing why appropriate consideration of privacy and civil liberties is important for a successful Insider Threat program. The Insider Threat program faces many challenges while attempting to protect national security and preserve an individual's rights, privacy, and civil liberties These challenges can be because of perceptions of intrusiveness, overreach, or questionable government activity. Insider Threat programs may encounter socially charged issues surrounding authorized and unauthorized disclosures, whistleblowing, protected speech, and threats of violence.

A popup appears on screen that lists the following lesson one objectives:

Lesson 3 Objectives

- Describe insider threat challenges related to unauthorized disclosure, whistleblowing, protected speech, and threats of violence not protected.
- Describe the difference between unauthorized disclosure and whistleblowing including whistleblower protections and protections against reprisal for reporting questionable government activity.
- Identify protected speech versus speech that is not protected (threats of violence).

Rachel: So the goal for today is to meet the objectives you see here. I will get with you in a little while to get started. Why don't you go to your office for now? I'll give you a call soon to discuss these matters.

Insider Threat Challenges

Screen 2 of 12

Text box appears, "Sometime later…"

Text box appears, "Select the phone to answer the call."

Insider Threat Challenges

Screen 3 of 12

Rachel: Hello, I thought we could start with one of our biggest challenges. Insider Threat programs must be careful to distinguish between unauthorized disclosures and whistle blowing

activities. They must also make sure that their actions do not impede exercise of free speech or constitutional liberties. Individuals may not be subject to Insider Threat program actions based on legally protected behavior or activity.

Therefore, by adhering to the use of accepted potential risk indicators and insider threat activities authorized under policy and regulation, our program can avoid infringing on an individual's rights and liberties as well as the perception that we are profiling or targeting individuals based on political beliefs, religious conviction, ethnicity, or other protected status.

I am about to email you something to help you clarify the difference between unauthorized disclosures and whistle blowing. I have to attend a meeting in a few minutes, but I will get with you after I'm finished.

The CDSE Unauthorized Disclosure Toolkit

Screen 4 of 12

Audio, "You have new Email."

Image of computer is highlighted in yellow.

Text box, "Select the computer to continue."

Email Text:

From: Rachel

Subject: The CDSE Unauthorized Disclosure Toolkit

Attachment: Whistleblower Protection Policies and FAQs

Hi,

Individuals with access to classified information have an obligation to protect it. Failure to do so can result in damage to national security and the warfighter. There are approved channels for the release and review of information prior to disclosure.

The Whistleblower Protection Act protects employees from direct retaliation for acts of reporting protected disclosures. There are also approved channels to report fraud, waste or other abuse through existing whistleblower or Inspector General channels.

One of our best resources is the DCSA CDSE Unauthorized Disclosure Toolkit. This toolkit will help you learn the difference between an unauthorized disclosure and whistleblowing, where and how to report both unauthorized disclosure and questionable government behavior and activities, and more.

It contains resources and links that will help you:

- Learn more about your responsibilities for safeguarding classified information

- Locate relevant policies and guidance
- Discover awareness materials
- Learn about prepublication procedures
- Appropriately report both unauthorized disclosure and questionable activities
- Properly respond to unauthorized disclosure events

For military members, whistleblowing is protected by 10 USC 1034, Protected Communications, which prohibits reprisals for making or preparing to make such communication such as taking or threatening to take an unfavorable personnel action or withholding or threatening to withhold a favorable personnel action. The No Fear Act protects federal employees from similar reprisals. We rely on whistleblowers to provide information as a source of allegations and as original and corroborating evidence. Federal employees within the Executive branch are required to report corruption. Whistleblowing is not a nice-to-have function; it is essential to the national security and defense mission of the Federal Government.

Keep in mind that there is a distinction between these actions and unauthorized disclosure. Unauthorized Disclosure occurs when there is communication or physical transfer of classified information or controlled unclassified information (CUI) to an unauthorized recipient. Unauthorized disclosure is not whistleblowing; it is a crime.

I attached a whistleblower protection policies and FAQ document to this email. It contains information and links that you may need to refer to when considering whistleblower protections.

VR,

Rachel

The Whistleblower Protection Policies and FAQs document is linked on screen.

What is Protected Speech?

Screen 5 of 12

Kendra: Hello, I thought I would stop by and see how you are doing with your training. Oh, I see you are reviewing some unauthorized disclosure and whistleblowing information. Good, since you are learning about that, this is a good time to talk about protected speech versus unprotected speech. Contrary to what many people think, public employees do not forfeit their constitutional rights by virtue of employment. We maintain our right to comment as a citizen about matters of public concern. However, not all speech is legally protected.

Statements generally not afforded First Amendment protection include those that:

- Reflect solely matters of internal or personal interest;
- Are false and defamatory statements about the Agency and/or Agency employees;
- Threaten and insult; including threats of violence;

Are “fighting words” that unduly disrupt the office, undermine a supervisor's authority, or destroy necessary close working relationships.

Protected Speech Activity

Screen 6 of 12

Kendra: I’m working on several cases that involve speech protections. So let’s try something. I will tell you a situation and you let me know which category of unprotected speech it belongs or if it is protected speech. Ok, let’s get started.

Kendra: This situation involves an employee who was reprimanded for not following security protocols. He started spreading rumors that the individual who reprimanded him was going to write up more people to justify their selection for a round of layoffs coming in the next six weeks.

Which type of unprotected First Amendment statement does this reflect?

Screen text displays the following:

An employee was reprimanded for not following security protocols. He started spreading rumors that the individual that reprimanded him was going to write up more people to justify their selection for a round of layoffs coming in the next six weeks.

Which type of speech would this situation fall?

A. Unprotected statement that unduly disrupt the office, undermine a supervisor's authority, or destroy necessary close working relationships
B. Unprotected statement that reflect solely on matters of internal or personal interest
C. Protected statement

Branch A - Screen text displays the following:
An employee was reprimanded for not following security protocols. He started spreading rumors that the individual who reprimanded him was going to write up more people to justify their selection for a round of layoffs coming in the next six weeks.
Which type of unprotected First Amendment statement does this reflect?

Unprotected statements that unduly disrupt the office, undermine a supervisor's authority, or destroy necessary close working relationships.

Kendra: You are correct. This statement is unprotected speech because it could cause undue panic in the workforce and weaken the supervisor’s ability to lead the organization.

Branch B - Screen text displays the following:
An employee was reprimanded for not following security protocols. He started spreading rumors that the individual that reprimanded him was going to write up more people to have justification for a round of layoffs coming in the next six weeks.

Which type of unprotected First Amendment statement does this reflect?

Unprotected statement that reflect solely on matters of internal or personal interest.

Kendra: OK, are you sure? I mean I agree it should fall under unprotected speech, but I do not see anywhere that the rumors were solely matters of internal or personal interest in the statement. It can be hard to determine if speech is interfering with a Supervisor or solely matters of internal or personal interest, because many of these situations are fact and workplace specific. We'll always work together to come to the appropriate decision on any legal aspects of insider threat matters. Branch C Scene opens in the student's office viewed from behind the desk. The desk has a computer, telephone, and inbox on it. Kendra is in the office.

Branch C -Screen text displays the following:
An employee was reprimanded for not following security protocols. He started spreading rumors that the individual that reprimanded him was going to write up more people to justify their selection for a round of layoffs coming in the next six weeks.

Which type of unprotected First Amendment statement does this reflect?

Protected statement.

Kendra: Hmmm…If I went in to a courtroom and suggested that the individual statements were protected, I think the judge would throw the book at me! But don't worry, we'll always work together to come to the appropriate decision on any legal aspects of insider threat matters.

Threats of Violence

Screen 7 of 12

Kendra: Ok now you know that some speech is not protected. Let's talk specifically about threats of violence and why they are not protected. The Supreme Court in R.A.V. v. City of St. Paul cited three reasons when threats of violence are not protected by the First Amendment.

This is due to the need to protect individuals from:

- The fear of violence;
- The disruption that fear engenders; and
- The possibility that the threatened violence will occur.

However, it has to be an actual threat, not a threat on a policy or one that encourages political action.

I placed a document in your in-box that contains links to the different laws and policies that discuss threats of violence. It's good information to have if you ever find yourself in a situation

involving threats of violence. Oh! Rachel wanted me to let you know we will be meeting in the conference room in a few minutes. See you there.

The Why Threats of Violence are Not Protected document is linked on screen.

The "Even-handedness Approach" and Insider Threat Programs

Screen 8 of 12

Screen text displayed: "In the Conference Room"

Screen text displayed: The "Even-handedness Approach"

Rachel: Good afternoon everyone! I called you all here to talk about the "Even-handedness Approach" and our Insider Threat Program. Even-handedness is a principle we must consider when conducting our Insider Threat Program activities such as user activity monitoring and incident response.

"Even-handedness" in development of process means that it is conduct that is under scrutiny, not individuals.

Triggers set for electronic monitoring and for reporting of behavior must be consistent with the adjudicative standards against which the particular behavior is measured.

What is the "Even-handedness Approach" and how is it applied to our program? Well, as it states on screen, our program's activities need to focus on conduct not individuals. In other words, our actions cannot be based on discriminatory criteria or motivated by personal bias. The monitoring of information by the Insider Threat Hub is not considered an unreasonable intrusion into privacy because it is directed at conduct and not specifically targeting an individual. As such, our triggers need to be set based on the laws and policy that outline the standard.

Behaviors should not be monitored or reported if they are irrelevant to the determination to be made, however negative they may be.

The workforce needs to understand what kinds of matters to report; we do not want to generate a population of self-appointed vigilantes.

Actions must be based on policy.

So if there is no law, policy, or standard that covers a behavior than we should not engage. However, that does not mean we shouldn't look at behaviors that should be added to our guidance.

It is important to keep in mind that insider threat programs are not intelligence activities and therefore are not subject to intelligence oversight, policy, or regulations such as EO 12333 and DoDD 5148.13. However, the guidance provided may be useful in developing or guiding Insider Threat procedures and best practices for your organization.

Rachel: As this states, our program's actions are not subject to the same rules as intelligence activities. That does not mean we should ignore the intelligence oversight, policy, or regulations. We can use the practices and protections outlined in the intelligence oversight, policy, or regulations to guide our Insider Threat policies. In addition, Counterintelligence and Law Enforcement activities to whom you may report insider threat matters may be subject to intelligence oversight rules, policy, or regulations.

Well that's it. The Even-handedness Approach seems pretty simple. I would like our new analyst to meet me in my office. Thank you all for making time for this quick briefing. I hope you got something from it.

Scenario Knowledge Check 1

Screen 9 of 12

Rachel: Well, you are certainly getting a lot of information thrown at you. We talked about unauthorized disclosures, whistleblowing, protected speech, threats of violence, and the challenges Insider threat programs face concerning these items. You also just attended the briefing covering the "Even-handedness Approach." So before we go any further, let me ask you a few questions.

While reviewing monitoring activities that occurred in the past year, an insider threat analyst noticed that some of the activities were not covered by Insider Threat policies. When it was brought to the attention of the team, the cybersecurity analyst stated that the individuals being monitored were visiting the website of an outspoken and controversial political group that was not friendly to the current administration. After hearing this, the program manager told the analyst to stop all monitoring activities immediately. Why did the program manager tell the analyst to stop all monitoring activities?

An insider threat program from another organization discovered that security personnel were conducting random searches of the offices after normal work hours. When the practice was questioned, Security personnel referenced an older but detailed internal Insider Threat Security policy that stated the searches were authorized.

While reviewing monitoring activities that occurred in the past year, an insider threat analyst noticed that some of the activities were not covered by Insider Threat policies. When it was brought to the attention of the team, the cybersecurity analyst stated that the individuals being monitored were visiting the website of an outspoken and controversial political group that was not friendly to the current administration. After hearing this, the program manager told the analyst to stop all monitoring activities immediately.

Pop up screen text displayed:

Why did the program manager tell the analyst to stop all monitoring activities?

A. They did not adhere to accepted potential risk indicators

B. They adhered to accepted potential risk indicators
C. The activities did not impede exercise of free speech or constitutional liberties
D. They did not distinguish between unauthorized disclosures and whistle blowing activities

Scenario Knowledge Check 2

Screen 10 of 12

Rachel: Let's try this one. An individual came across an agency practice that was possibly illegal. After informing the supervisor and seeing no action, the individual reported the practice to the agency Inspector General's office. Once the agency halted the practice, the leadership attempted to revoke the individual's security clearance.

Are the agency's actions wrong and why?

Pop up screen text displayed:

An individual came across an agency practice that was possibly illegal. After informing the supervisor and seeing no action, the individual reported the practice to the agency Inspector General's office. Once agency halted the practice, the leadership attempted to revoke the individual's security clearance.

Are the agency's actions wrong and why?

A. Wrong. The individual is a whistleblower and protected because he reported through acceptable channels, in this case the Inspector General.
B. Wrong. The situation is a result of the agency leadership not addressing the possibly illegal practice
C. Not wrong. The agency's actions are in response to an unauthorized disclosure
D. Not wrong. The reporting individual failed to follow approved channels to report fraud, waste or other abuse

Scenario Knowledge Check 3

Screen 11 of 12

Rachel: Ok, last one I promise. While conducting an insider threat response, an analyst discovered information that was not connected to the incident. However, because the analyst, felt the information indicated the individual was "Anti-American," he included the information in his reports. What portion of the "Even-handedness Approach" did the analyst fail to consider?

Pop up screen text displayed:

While conducting an insider threat response, an analyst discovered information that was not connected to the incident. However, because the analyst, felt the alleged information indicated the individual was "Anti-American," he included the information in his reports.

What portion of the "Even-handedness Approach" did the analyst fail to consider if any?

A. Behaviors should not be monitored or reported if they are irrelevant to the determination being made.
B. Triggers must be consistent with the adjudicative standards.
C. Actions must be based on the evidence discovered.
D. These are intelligence activities and therefore subject to intelligence oversight.

Day Three in the Books

Screen 12 of 12

Rachel: You are definitely picking this up quickly.

We talked about the challenges we face concerning unauthorized disclosures versus whistleblowing and the differences between the two. Then we covered what is protected and unprotected speech, and finally we discussed the "Even-handedness Approach."

Let's stop for today. We can start up again tomorrow by discussing balancing institutional protections and individuals' rights.

Balancing Institutional Protections and Individuals' Rights Lesson

The Morning, Final Training Day

Screen 1 of 11

Pop up screen text displayed:

Lesson 4 Objectives

- Identify collaborative roles associated with privacy and civil liberties that are critical to the Insider Threat Program.
- Identify potential conflicts between the Insider Threat Program procedures and organization policies.

Collaborative Roles Meeting Invitation

Screen 2 of 11

Screen text, "In your Office"

Audio, "You have new Email."

Image of computer is highlighted in yellow.

Screen text, “Select the computer to continue.”

From: Rachel

Subject: Team Meeting

Good Morning Team,

I would like us to all meet in the conference room in a few minutes. Thanks.

VR,

Rachel

Collaborative Roles

Screen 3 of 11

Screen text displayed: “In the Conference Room”

Screen text displayed: Team Roles Associated with Privacy and Civil Liberties

Select a team member

Rachel: Good morning everyone! It’s good to see you all. As I was on my way out the door yesterday, it dawned on me that we have not shared one of our greatest privacy and civil liberties resources with our new analyst—our own Insider Threat team. Each role associated with the team has been carefully selected for the skills and knowledge they bring to the team. I figured our new analyst could benefit from hearing each team member. Could each of you explain your involvement in regards to privacy and civil liberties?

When Kendra is selected, an ID card with a picture of Kendra displays. On the card the text reads, Kendra Legal Counsel

Kendra: Ok, as you already know, I am the team’s attorney. When it comes to privacy and civil liberties concerns, I am the primary role player. The legal guidance I give should assist all other team members as they execute actions for the insider threat program. I can also help determine if the policies and procedures established by our Insider Threat Senior Official or Program Manager comply with policy and regulation. If you have a privacy and civil liberties issue, make sure you get with me as soon as you can.

When Evan is selected, an ID card with a picture of Evan displays. On the card the text reads, Evan Human Resources

Evan: As a Human Resource Specialist working with employee assistance programs, I encounter a lot personal information, including yours. So, I am very familiar with the protection of

personally identifiable information or PII. Let me know if you have any questions, I'll be glad to help.

When Layla is selected, an ID card with a picture of Layla displays. On the card the text reads, Layla Behavioral Science

Layla: I am the team's Behavioral Science Specialist. My role involves identifying, describing, and documenting the types of risky behavior and conduct that an insider analyst looks for. I also make sure triggers and indicators focus on conduct and not on individual characteristics such as race, gender, sexual orientation, or constitutionally protected activity. Also, like Evan, I'm extremely familiar with protected health information or PHI. So, if you have concerns with PHI or HIPAA, I may be able to help you.

When Connor is selected, an ID card with a picture of Connor displays. On the card the text reads, Connor Physical Security

Connor: Security managers play a role in certain insider threat program actions that may involve privacy and civil liberties issues. We have contact with individuals or their belongings, which may involve searches. So, the team works with legal and meme to establish acceptable protocols for the program.

When Trinity is selected, an ID card with a picture of Trinity displays. On the card the text reads, Trinity Cybersecurity Specialist

Trinity: As a Cybersecurity Specialist, I play a role in certain insider threat program actions that involve authorized monitoring of information-system-user activity. . I work with the team, especially legal, to establish protocols for the program, including making certain that we placed banners appropriately on information systems subject to monitoring.

When Ethan is selected, an ID card with a picture of Ethan displays. On the card the text reads, Kendra Counter intelligence

Ethan: Counterintelligence personnel are familiar with intelligence oversight regulations. As you already know, insider threat programs are not intelligence activities and therefore not subject to Intelligence Oversight under Executive Order 12333. However, we are knowledgeable about these protections and take them seriously. We can assist legal counsel and the team when determining whether an activity constitutes unauthorized disclosure or the authorized reporting of questionable government activities as well as issues relating to criminal conduct.

When Aaron is selected, an ID card with a picture of Aaron displays. On the card the text reads, Aaron Law Enforcement

Arron: Law enforcement takes the lead when it comes to investigating and apprehending individuals suspected of criminal activity. We are highly trained in conducting investigations and collecting evidence while maintaining an individual's privacy and liberties. We work with legal, counterintelligence, security, and the rest of the team to ensure personnel that pose an insider threat are brought to justice.

Collaborative Roles, Cont.

Screen 4 of 11

Screen text displays the following:

Team Roles Associated with Privacy and Civil Liberties

Rachel: So now that you know the roles we have on our team, you will need to work with our team members and legal counsel to ensure that we appropriately access, store, and retain information.

Evan, I would like you to make some time to discuss potential conflicts between the Insider Threat Program procedures and organization policies with our new analyst. Thank you for your time everyone.

Maintaining and Sharing Conflicts

Screen 5 of 11

Screen text, "Evan's Office"

Evan: The first area we need to discuss is Maintaining and sharing of personal records and information. This area that can lead to conflict. Individual employees may not want to report to the Insider Threat Office because they are afraid of getting in trouble for sharing information or that the person they are reporting will have their rights violated. Supervisors and managers may be hesitant to share with the Insider Threat Program office because they have learned not to share PII. Human Resources offices often refuse to share PII with insider threat programs. They may need a reminder that insider threat program personnel may lawfully access this information by virtue of their position.
The tool I gave you discusses this in the Policies and Practices to Mitigate Insider Risk section. Be sure to read it when you have some time.

Evan: Hello. Rachel wanted me to get with you to discuss potential conflicts between Insider Threat procedures and organization policies. Insider threat programs are designed to deter, detect, and mitigate risks associated with insider threats. Law, policy, and regulation require our program to conduct certain activities to achieve the mission. Sometimes this can lead to conflict in an organization when some departments don't understand the purpose and authorities of the insider threat program. I have the PERSEREC Insider Risk Evaluation and Audit Tool for you to refer to as we talk about these potential conflicts. Go ahead and grab it from my desk. Don't worry if you close it. You can get it from your resources tab at any time.

The Insider Risk Evaluation and Audit Tool document is linked on the screen.

Reporting and Monitoring Procedure Conflicts

Screen 6 of 11

Evan: Another area related to maintaining and sharing information is reporting procedures and requirements. Both require some level of sharing of information. People are not sure what or where to report. You must have protocols in place for securely reporting or referring insider threat matters as part of your mitigation response. Again, the Policies and Practices to Mitigate Insider Risk section discuss this.

Evan: User monitoring is a potential point of conflict because there can still be expectations of privacy and protected information even in monitored environments. See the Policies and Practices to Mitigate Insider Risk section for more on monitoring.

Employee Termination and Reprimanding Procedure Conflicts

Screen 7 of 11

Evan: Another issue that comes up is that employee termination and reprimand procedures may cause conflict with supervisors, managers, and commanders who may have been used to taking these actions unilaterally without realizing the result and unintended consequences. See the Management Intervention: Assessment and Planning section of the PERSEREC Insider Risk Evaluation and Audit Tool for more on this topic. Pay particular attention to the paragraph preceding Table 7, Management Intervention.

Pop up screen text displayed: Select the document on the desk.

Evan: So how do you manage these conflicts? One of the best ways is through your Insider Threat Hub personnel. There should be a representative from each of these elements – cyber, counterintelligence, HR, security, and more - on the Hub team. These folks are the experts in their particular areas and they know the purpose and authorities of the Insider Threat Program. They can help you advocate for your program and assist in developing a relationship with these elements of your organization. They can also assist in the establishment of appropriate procedures so that these elements can give you information according to proper authorities.

You should also be sure to get buy-in from the Office of General Counsel on the actions you are taking. They can help explain your authorities to other elements of your organization. It’s also very important that senior leadership understands the Insider Threat Program is an integral part of the organization and makes sure that the other directorates are cooperative. The Insider Threat Senior Official plays a crucial role in maintaining these relationships with the general counsel and leadership.

Remember resolving conflict in all of these cases is essential. Everyone on the Insider Threat team should be able to explain the program, our authorities, and mission. We often hold information sessions to educate the other directorates on our program and it really seems to help.

I will say that having legal and senior leadership buy-in for these events has been the key to our success.

Thanks for coming over and talking about these potential conflicts before you find yourself in the middle of one. Oh, I just got an email from Rachel; she wants to see you in her office.

The Insider Risk Evaluation and Audit Tool document is linked on the screen.

Workplace Environment and Organizational Justice

Screen 8 of 11

Rachel: Hey! I hope the meeting with Evan shed some light on how procedures can be a source of conflict because it feeds into what we need to talk about now. Organizational justice in the workplace is an issue that should concern all of us. Hostile or negative work environments can lead to disgruntlement. And some disgruntled employees may commit crimes against their employers, possibly in the form of fraud, embezzlement, espionage, and sabotage. Even violence has resulted in extreme cases. Nevertheless, we can take steps to mitigate risks by employing principles of organizational justice. The principles include ensuring our policy, procedures, and treatment of employees are perceived as fair; that we respect privacy and civil liberties; and by engaging the workforce in a positive manner. These principles will foster a more positive workplace environment, thereby lowering risk. Exhibiting these principles of organizational justice and evenhandedness also helps cast a positive light on our Insider Threat Program.

Here, I put together some information for you on organizational justice. It’s a good idea to keep them in the back of your mind when performing your duties.

Let’s go to the Conference room and meet up with the rest of the team

Pop up screen text displayed: Select the document on the desk.

The Workplace Environment and Organizational Justice document is linked on the screen.

Scenario Knowledge Check 1

Screen 9 of 11

Rachel: Good to see you all again. Our new analyst has covered a lot of information today We discussed the team roles associated with privacy and civil liberties, and the sometimes conflicting Insider Threat procedures and organization policies. We also talked about organizational justice. So, before we head for home, I wanted to bring the team together to ask our new analyst a few questions. Who would like to start?

Layla: Hey Rachel, I have one. Our team was working with security to develop a protocol for conducting random inspections of vehicles entering their facility. While developing the procedure, the analyst consulted with law enforcement and the General Counsel. With whom

should the team consult prior to giving the protocol to the Insider Threat Program Manager to get leadership buy-in?

Pop up screen text displayed:

Our team was working with security to develop a protocol for conducting random inspections of vehicles entering their facility. While developing the procedure, the analyst consulted with law enforcement and the General Counsel.

At a minimum, with whom should the analyst consult prior to giving the protocol to the Insider Threat Program Manager to get leadership buy-in?

A. Physical Security and Human Resources
B. None. Only consult LE and Legal
C. Counterintelligence only
D. Cybersecurity only

Scenario Knowledge Check 2

Screen 10 of 11

Screen text: Team Roles Associated with Privacy and Civil Liberties

Rachel: That was a good one Layla! Good job. Let's try one more. Evan, do you have question for our new analyst?

Evan: Hey Rachel, I have one. An Insider Threat team worked diligently on resolving threats posed by the exfiltration of classified or sensitive information by insiders. As a countermeasure, they asked the IT team to change some procedures that included stricter limits on the size of email attachments. They implemented the limits immediately. The team notified the workforce of the change in an email message and informed them it was required by insider threat program policy. Within a day of the change, management received multiple complaints from the workforce that they could no longer perform their duties due to the restrictions. Which portion of resolving conflicts with Insider Threat procedures and organization policies did the team neglect to accomplish?

Pop up screen text displayed:

An Insider Threat team worked diligently on resolving threats posed by the exfiltration of classified or sensitive information by insiders. As a countermeasure, they asked the IT team to change some procedures that included stricter limits on the size of email attachments. They implemented the limits immediately. The team notified the workforce of the change in an email message and informed them it was required by insider threat program policy. Within a day of the change, management received multiple complaints from the workforce that they could no longer perform their duties due to the restrictions.

Which portion of resolving conflicts with Insider Threat procedures and organization policies did the team neglect to accomplish?

A. Failed to consider the impact on the mission
B. Failed to consider civil liberties
C. Failed to conduct in proper information sharing
D. Failed to ensure protocols were in place for securely reporting

End of the Day

Screen 11 of 11

Rachel: Excellent questions team! I think our new analyst is ready to handle most privacy and civil liberty issues, or at a minimum, knows whom to call to help with those issues.

We talked about the collaborative roles we have on our team and discussed conflicts between the Insider Threat Program procedures and organization policies. I think you will definitely be an asset to our team.

Course Conclusion

Course Summary

Screen 1 of 3

A collage of images used throughout the course slowly fading in and out as narration plays.

Narrator: As an insider threat program team member, it is your responsibility to make sure your actions do not infringe on an individual's legal privacy and civil liberties.

This course has provided you with the basic tools and information to ensure your Insider Threat Program considers privacy and civil liberties concerns and balances them against the interests of national security.

Your organization may have additional policies and procedures related to privacy, civil rights, and civil liberties. Review your Insider Threat Program's directives, instructions, delegations, guidance, and SOPs periodically. And remember to consult with your legal team, including privacy officials and office of general counsel representatives, when you have questions.

Course Objectives

Screen 2 of 3

Image of the Constitution of the United States of America.

Narrator: Congratulations, you have completed the Privacy and Civil Liberties Overview course. You should now be able to perform the listed activities. To receive credit for this course, you must take the Privacy and Civil Liberties Overview examination.

Screen text displayed:

Privacy and Civil Liberties Overview Course Objectives*:*

- Given instruction, the student will be able to identify federal laws, policies, and regulations that ensure privacy and civil liberties.
- Given instruction, the student will be able to explain why appropriate consideration of civil liberties and privacy is important for a successful insider threat program.
- Given instruction, the student will be able to explain insider threat challenges impacted by socially charged matters regarding civil liberty laws and policies.
- Given instruction, the student will be able to explain how to implement institutional protections within an insider threat program that maintain a proper balance between security practices and individuals' liberty and privacy interests.

Course Examination

Screen 3 of 3

A box appears on the screen that reads:

To receive course credit, you must take the course examination. Select the Take Examination button to launch the online exam.

Take Exam button

This page intentionally left blank.

Answer Key
Privacy and Civil Liberties Overview

Privacy and Civil Liberties Guidelines

Scenario Knowledge Check 1

Of the items listed, which should the team highlight as PII? Select all that apply.

A. Social Security Number
B. Address
C. Name
D. Position Description

Answer:

The term Personally Identifiable Information refers to information used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Civil Liberties, and Insider Threat Programs

Scenario Knowledge Check 1

Which step of the OPSEC process would the analyst apply in this situation?

A. Analysis of vulnerabilities
B. Analysis of threats
C. Assessment of risks
D. Application of appropriate countermeasures

Answer:

Vulnerability analysis requires that the adoption of an adversarial view of the activity requiring protection. The analyst attempts to identify weaknesses or susceptibilities that can exploited by the adversary's collection capabilities.

Which part of the principle of confidentiality was not taken into consideration in this situation?

A. Preventing negligent damaging of an individual's reputation
B. The Privacy Act of 1974
C. Cybersecurity and information sharing

D. Treating the workforce with fairness

Answer:

It is important to prevent any negligent damaging of an individual's reputation or professional status. If an error results in harm to an individual's prospects for continued employment or future employment, redress must be afforded.

Insider Threat Challenges with Privacy and Civil Liberties

Scenario Knowledge Check 1

Why did the program manager tell the analyst to stop all monitoring activities?

A. They did not adhere to accepted potential risk indicators
B. They adhered to accepted potential risk indicators
C. The activities did not impede exercise of free speech or constitutional liberties
D. They did not distinguish between unauthorized disclosures and whistle blowing activities

Answer:

By adhering to accepted potential risk indicators and insider threat activities authorized under policy and regulation, programs can avoid impinging on individual rights and liberties as well as to prohibit the actual or perceived profiling or targeting of individuals based on rightfully held political beliefs, religious conviction, ethnicity, or other protected status.

Scenario Knowledge Check 2

Are the agency's actions wrong and why?

A. Wrong. The individual is a whistleblower and protected because he reported through acceptable channels, in this case the Inspector General.
B. Wrong. The situation is a result of the agency leadership not addressing the possibly illegal practice
C. Not wrong. The agency's actions are in response to an unauthorized disclosure
D. Not wrong. The reporting individual failed to follow approved channels to report fraud, waste or other abuse

Answer:

The actions of the agency are clearly wrong. Whistleblowers are protected from reprisals by 10 USC 1034.

Scenario Knowledge Check 3

What portion of the "Even-handedness Approach" did the analyst fail to consider if any?

A. Behaviors should not be monitored or reported if they are irrelevant to the determination being made.
B. Triggers must be consistent with the adjudicative standards.
C. Actions must be based on the evidence discovered.
D. These are intelligence activities and therefore subject to intelligence oversight.

Answer:

The "Even-handedness Approach" states behaviors should not be monitored or reported if they are irrelevant to the determination being made.

Balancing Institutional Protections and Individuals' Rights

Scenario Knowledge Check 1

At a minimum, with whom should the analyst consult prior to giving the protocol to the Insider Threat Program Manager to get leadership buy-in?

A. Physical Security and Human Resources
B. None. Only consult LE and Legal
C. Counterintelligence only
D. Cybersecurity only

Answer:

The analyst should consult with Physical Security and Human Resources next to establish accepted protocols for the program.

Scenario Knowledge Check 2

Which portion of resolving conflicts with Insider Threat procedures and organization policies did the team neglect to accomplish?

A. Failed to consider the impact on the mission
B. Failed to consider civil liberties
C. Failed to conduct in proper information sharing
D. Failed to ensure protocols were in place for securely reporting

Answer:

The team failed to consider the impact on the mission.