Introduction to Personnel Security

Student Guide

April 2024

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Course Introduction

Course Overview

Welcome to the Introduction to Personnel Security course. This course provides an overview of the Department of Defense Personnel Security Program (PSP). During this course, you will learn about key elements and considerations of the PSP, including position designation, investigative standards, adjudicative requirements, and the responsibilities and duties of security professionals.

Here are the course objectives.

- Summarize the key elements of personnel security.
- Through given scenarios, assess the requirements for successful and accurate position designation, including the sensitivity levels of positions and any potential adverse effects on national security.
- Apply the Federal Personnel Vetting Investigative Standards and adjudications under TW 2.0 to a series of situational examples involving personnel.
- Apply the adjudication requirements for national security eligibility determinations through given scenarios involving military, contractors, and civilian personnel.
- Distinguish the security professional's responsibilities and duties in accordance with the Personnel Security Program (PSP) through given situations and scenarios.

Optional Test-Out

You have the option to demonstrate your proficiency in the course's subject matter by successfully completing a pre-test prior to going through the course content (this is the "test out option").

The pre-test is divided into sections. Each section corresponds to a lesson in this course.

If you choose to take the pre-test, and you pass a section with a minimum score of 80%, you will not be required to take the corresponding lesson for that section.

If you fail to pass a section on the pre-test, you will be required to complete that lesson of this course.

If you wish to complete the test-out option, please access the course through the Security Training, Education, and Professionalization Portal (STEPP).

Lesson 2: Overview of Personnel Security

Introduction

Lesson Objectives

This lesson will provide an overview of personnel security, including an introduction to the Personnel Security Program, Trusted Workforce 2.0, and Continuous Vetting. It will also look at the evolution of personnel security through time, including the Executive Orders, policies, regulations, and guidelines that have shaped it.

Here are the lesson objectives.

- Identify the primary components of the Personnel Security Program (PSP).
- Define the Trusted Workforce (TW) 2.0 framework and identify its key improvements in the reform of the personnel security process and establishment of a single vetting system.
- Identify continuous evaluation (CE) and continuous vetting (CV) requirements.
- Identify the key Executive Orders, policies, regulations, and guidelines that influence the personnel security methodology.

Overview of the PSP

Purpose of the PSP

The Personnel Security Program (PSP) aims to protect national security by ensuring that only loyal, trustworthy, and reliable individuals may access classified information and/or be assigned to national security sensitive positions. The PSP establishes the standards, criteria, and guidelines upon which personnel security trust determinations are based. It uses a continuous and comprehensive background investigative process to support this determination.

The PSP applies to members of the Armed Forces, Department of Defense (DOD) civilian employees, DOD contractors, and other affiliated people who require access to classified information or who are assigned national security sensitive duties.

Personnel Vetting vs. Personnel Security

So, what is the difference between personnel vetting and personnel security?

The federal personnel vetting program encompasses all vetting domains including suitability, fitness, national security, and credentialing.

Personnel security refers to the national security domain, and consists of three distinct processes: background investigations, adjudications, and continuous vetting. This course primarily focuses on personnel security, which is the national security component of personnel vetting.

Access to Classified Information

Let's take a closer look at two key aspects of the PSP.

The first aspect is providing access to classified information. Unauthorized disclosure of classified or sensitive information can cause significant harm to national security. Information that requires special protection is known as classified national security information (CNSI). In the U.S., there are three levels of classified information: Top Secret, Secret, and Confidential. The degree of damage to national security that could result from its unauthorized disclosure determines which classification applies. Top Secret is the highest level of classification. It applies to information that reasonably could be expected to cause exceptionally grave damage to the national security if unauthorized disclosure occurs. Secret classification applies to information that could be expected to cause serious damage to the national security if unauthorized disclosure occurs. Confidential classification applies to information that reasonably could be expected to cause damage to the national security if unauthorized disclosure occurs.

National Security

The second key aspect of the PSP is ensuring the protection of national security. National security encompasses both the national defense and the foreign relations of the U.S. which must be protected from harmful individuals, organizations, and nations. One way a nation can defend itself is to maintain a good working relationship with other countries, thereby reducing threats to our nation's survival. Unfortunately, some national security threats faced by the U.S. come from individuals who are trusted insiders. These are known as insider threats. Therefore, assigning individuals who possess a history of being loyal, trustworthy, and reliable to sensitive positions is critical to protecting and maintaining our national security.

Review Activity 1

Which of the following are key aspects of the Personnel Security Program (PSP)?

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

- ☐ Overseeing the competitive hiring system.
- ☐ Providing eligibility to access classified information.
- ☐ Ensuring the protection of national security.
- ☐ Managing the auditing of defense contractors.

Review Activity 2

Which of the following are processes of personnel security?

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

- ○ Background investigations
- ○ Adjudications
- ○ Continuous vetting
- ○ All of the above

Background and History

History of the PSP

To understand the personnel security methods of today, it is important to look at the background and history of personnel security and how it has evolved, and continues to evolve. Let's take a brief look at the origins of personnel security starting with the spoils system introduced in 1828, to the Civil Service Act of 1883, and the Hatch Act of 1939.

Spoils System

When Andrew Jackson was president, he fired twenty percent of federal officials and put in his supporters that helped him during the election of 1828. This was known as the Spoils System. The Spoils System was the system by which people were appointed to civil service jobs. This system required allegiance to the party boss and the political party that appointed you, as opposed to a larger sense of allegiance to the Constitution. The meaning of the Spoils System was to give appointive jobs to loyal members of the party in power. Because of the many abuses of the Spoils System, such as incompetent and corrupt political officials, or civil servants who felt they were working for the party rather than the American people, Congress passed the Civil Service Act in 1883.

Civil Service Act

Prior to the Civil Service Act of 1883, federal employees, even at the lowest levels, were political appointees. Considered to be the "Magna Carta" of civil service reform, the Civil Service Act created the U.S. Civil Service Commission. The act required employees to be appointed based on ability, which was demonstrated by taking an exam. This created uncertainty about the partisan allegiance of federal employees who were no longer dependent upon the party favor to keep their jobs. Their party loyalty could no longer be "bought" or necessarily even depended upon.

Hatch Act

Eventually, Congress passed the Hatch Act of 1939, which limited certain political activities of federal employees. It ensured administration of federal programs in a nonpartisan fashion. Moreover, the Hatch Act protected federal employees from political coercion in the workplace. It made certain that federal employees receive advancement based on merit and not based on political affiliation.

Key Executive Orders, Policies, Regulations, and Guidelines

Executive Orders

Having reviewed the background and history of personnel security, now let's look at the applicable policies. The PSP is governed by several Executive Orders (E.O.s).

E.O. 10450, Security Requirements for Government Employment (Apr. 27, 1953)

- Requires that all persons who are employed by the departments and agencies of the government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States.
- Establishes security requirements for government employment. Each civilian officer or employee in any department or agency of the government shall be made subject to investigation.
- The scope of the investigation shall be determined in the first instance according to the degree of adverse effect the occupant of the position sought to be filled could bring about, by virtue of the nature of the position, on the national security.

E.O. 10865, Safeguarding Classified Information within Industry (Feb. 20, 1960)

- Provides for due process for industry applicants.

E.O. 12968, Access to Classified Information and Background Investigative Standards (Aug. 2, 1995)

- Establishes a uniform federal Personnel Security Program for employees who are considered for initial or continued access to classified information.
- This order also establishes security policies designed to protect classified information.

E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (Jun. 30, 2008)

- Requires an aligned system for all vetting domains.
- Established the Security Executive Agent (SecEA) role, and designated the Director of National Intelligence (DNI) as the SecEA.
- Established the function of oversight of investigations and determinations of eligibility for access to classified information or to hold a sensitive position.
- Requires Continuous Evaluation (CE).

E.O. 13764, Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters (Jan. 17, 2017)

- Amends E.O. 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information" (Jun. 30, 2008) and E.O. 13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust" (Jan. 16, 2009).
- Modernizes the executive branch enterprise to ensure all persons performing work for, or on behalf of the government, are and continue to be loyal to the United States, reliable, trustworthy, and of good conduct and character, and use mutually consistent standards and procedures.

E.O. 13869, Transferring Responsibility for Background Investigations to the Department of Defense (Apr. 24, 2019)

- Transfers the National Background Investigations Bureau (NBIB) investigative functions, personnel and resources to the DOD/ DCSA.

SEADS

There are several Security Executive Agency Directives (SEADs) that are important in governing the PSP.

SEAD 2: Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position (Revised Sep. 1, 2020)

- Establishes policy and assigns responsibilities governing the use of polygraph examinations conducted by agencies in support of personnel security vetting for initial or continued eligibility for access to classified information, or eligibility to hold a sensitive position.
- SEAD 2 only applies to a small subset of personnel vetting subjects.

SEAD 3: Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position (Jun. 12, 2017)

- Establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position.
- This directive does not limit the authority of agency heads to impose additional reporting requirements in accordance with their respective authorities under law or regulation.

SEAD 4: National Security Adjudicative Guidelines (Jun. 8, 2017)

- Establishes the single, common adjudicative criteria for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.
- National Security Guidelines contained in SEAD 4 supersede all previously issued national security adjudicative criteria or guidelines.

SEAD 5: Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications (May 12, 2016)

- Provides guidance for the collection and use of publicly available social media information during the conduct of personnel security background investigations and adjudications for determining initial or continued eligibility for retention of such information.

SEAD 6: Continuous Evaluation (CE) (Jan. 12, 2018)

- Establishes policy and requirements for the CE of individuals who require continued eligibility for access to classified information or eligibility to hold a sensitive position.
- CE modernizes the background investigation process by maximizing automated records checks to identify adjudicative relevant information to assist in assessing the continued eligibility of individuals at any time during their period of eligibility.

SEAD 7: Reciprocity of Background Investigations and National Security Adjudications (Nov. 9, 2018)

- Establishes requirements for reciprocal acceptance of background investigation and national security adjudications for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

SEAD 8: Temporary Eligibility (May 18, 2020)

- Establishes policy and requirements for authorizing temporary, often referred to as "interim," eligibility.
- It includes temporary access to classified information, temporary access to a higher level of classified information, one-time access to classified information, temporary eligibility to hold a sensitive position, and temporary eligibility to hold a higher level sensitive position when determined to be in the national security interest.

SEAD 9: Whistleblower Protection: Appellate Review of Retaliation Regarding Security Clearances and Access Determinations (May 28, 2022)

- Establishes policy for the Director of National Intelligence's (DNI) appellate review process for employees who seek to appeal an adverse final agency determination with respect to alleged retaliatory action(s) taken by an employing agency affecting the employee's security clearance or access determination as a result of protected disclosures.

DOD Regulations

The implementation of the PSP within DOD is guided by DOD Instruction (DODI) 5200.02, DOD Personnel Security Program and DOD Manual (DODM) 5200.02, Procedures for the DOD Personnel Security Program.

DODI 5200.02 establishes policies, assigns responsibilities, and prescribes procedures for the DOD PSP.

DODM 5200.02 implements policy, assigns responsibilities, and provides procedures for the DOD PSP. This issuance assigns responsibilities and prescribes procedures for investigations of individuals seeking to hold national security positions or perform national security duties. The manual also sets procedures for DOD national security eligibility for access determinations; personnel security actions; continuous evaluation (CE); and security education requirements for employees seeking eligibility for access to classified information or to hold a sensitive position.

FPV Core Doctrine

Released jointly by the Office of Personnel Management (OPM) as the suitability and credentialing executive agent, and DNI as the security executive agent, the Federal Personnel Vetting (FPV) Core Doctrine guides the transformative efforts to reform the U.S. government personnel security vetting process. It aligns the federal workforce vetting processes to: promote mobility, improve efficiencies, and move towards an enhanced risk management approach.

Review Activity 3

Question 1 of 2. Which of the following Executive Orders (E.O.s) requires all persons who are employed by the government to be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States?

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

- ○ E.O. 10450, Security Requirements for Government Employment
- ○ E.O. 10865, Safeguarding Classified Information within Industry
- ○ E.O. 13764, Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters
- ○ E.O. 13869, Transferring Responsibility for Background Investigations to the Department of Defense

Question 2 of 2. Which of the following Executive Orders (E.O.s) amends E.O. 13467 and E.O. 13488?

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

- ○ E.O. 10450, Security Requirements for Government Employment
- ○ E.O. 10865, Safeguarding Classified Information within Industry
- ○ E.O. 13764, Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters
- ○ E.O. 13869, Transferring Responsibility for Background Investigations to the Department of Defense

Review Activity 4

Which of the following policy documents guides the transformative efforts to reform the U.S government personnel security vetting process?

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

- ○ DOD Instruction (DODI) 5200.02, DOD Personnel Security Program
- ○ DOD Manual 5200.02 (DODM), Procedures for the DOD Personnel Security Program.
- ○ Federal Personnel Vetting (FPV) Core Doctrine
- ○ Security Executive Agency Directive (SEAD) 6: Continuous Evaluation (CE)

Overview of TW 2.0

What is TW 2.0?

Now that we've looked at the history of the PSP and key policies, let's look at today's operations including an overview of Trusted Workforce (TW) 2.0.

Today's end-to-end personnel vetting operations includes: the Federal Personnel Vetting background investigations program, trust determinations, which are previously referred to as adjudications, continuous vetting, and insider threat analysis. TW 2.0 is the whole-of-government approach to reforming the personnel security process. TW 2.0 establishes a single vetting system for the U.S. Government. Implementation began in 2018, following extensive planning and interagency coordination. This revamped vetting focuses on mission needs, outlining five specific vetting scenarios under one policy framework. We will cover these in detail later in the course.

Improvements under TW 2.0

Several improvements are made under TW 2.0 including reducing the time required to onboard new hires, simplifying workforce mobility, enhancing risk management by identifying potentially problematic behavior sooner than traditional vetting tools and processes, and improving the ability of personnel vetting programs to meet agency mission needs while considering unique agency-specific requirements.

TW 2.0 Technology

Furthermore, TW 2.0 provides secure end-to-end information technology (IT). The personnel vetting ecosystem includes a suite of IT shared services. Many of these are already operational today as part of the suite of IT operated by the Defense Counterintelligence and Security Agency (DCSA). These services include:

- Electronic Application, known as eAPP, which has replaced Electronic Questionnaires for Investigations Processing, known as e-QIP
- The Position Designation Tool (PDT)
- The Central Verification System (CVS)
- The Defense Information System for Security (DISS)

As DCSA deploys the National Background Investigation Services (NBIS) IT shared services will be migrated to the new technology. NBIS is the new personnel vetting IT system. This will transform the vetting process to deliver stronger security, faster processing, and better information sharing. It replaces a suite of outdated, legacy IT systems. NBIS is the future of personnel vetting, as it enables the federal government to fully meet necessary TW 2.0 policy reforms.

Review Activity 5

Which of the following describes the purpose of TW 2.0?

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

- ☐ It provides a whole-of-government approach to reforming the personnel security process.
- ☐ It provides a one phase process for onboarding federal contractors.
- ☐ It establishes a single vetting system for the U.S. government.
- ☐ It revises the adjudication guidelines applied for national security purposes.

Review Activity 6

Which of the following are key improvements under TW 2.0?

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

- ☐ Reducing time required to onboard new hires.
- ☐ Simplifying workforce mobility.
- ☐ Enhancing risk management.
- ☐ Providing a universal approach to agency needs.

CV Overview and Methodology

Overview of CV

Next, we will provide a quick overview of continuous vetting (CV), which is a key change in the evolution of personnel vetting under TW 2.0. We will examine to whom CV applies, what CV is, why CV is done, and how CV is done.

Who does CV apply to?

CV applies to individuals with Federal government affiliation who are eligible for access and signed a Standard Form 86 (SF-86), dated 2010 or later.

What is CV?

CV, as defined by the 2017 E.O. 13764, is the process of reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements. Vetting policies and procedures are further sustained by an enhanced risk-management approach that facilitates early detection of issues. CV is a near real-time review of an individual's background at any time to determine if they continue to meet their requirements to uphold eligibility to access classified information. Note that access is the ability and opportunity to gain knowledge of classified information. Unlike its Continuing Evaluation (CE) predecessor, CV replaced periodic reinvestigations with an improved risk management approach that continually assesses workforce behaviors.

Why is CV done?

The goal of CV is early detection. That is, CV addresses potential risk indicators early on, allowing individuals the opportunity to seek assistance and mitigate issues before becoming an insider threat.

How is CV done?

CV is done through automated records checks to address seven data categories, agency-specific checks, and event and time-driven checks.

CV Process

Let's take a closer look at the CV process.

Automated record checks pull data from criminal, terrorism, and financial databases, as well as public records, at any time during an individual's period of eligibility. When DCSA receives an alert, it assesses whether the alert is valid and worthy of further investigation. DCSA investigators and adjudicators then gather facts and make eligibility determinations. CV helps DCSA mitigate personnel security situations before they become larger problems, either by working with the cleared individual to mitigate potential issues, or in some cases suspending or revoking eligibility.

Comparing CE, CV, and TW 2.0

CE, CV, and TW 2.0

Now, let's compare the key principles of CE, CV, and TW 2.0.

CE is a vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to assist in the ongoing assessment of an individual's continued eligibility. CE is intended to complement CV efforts.

CV is a robust and near real-time review of a covered individual's background at any time to determine whether that individual continues to meet applicable requirements. It replaced periodic reinvestigations with ongoing, and often automated, assessments of a person's security risk. CV offers an improved risk management approach that continually assesses workforce behaviors.

TW 2.0 is an enterprise approach to overhaul the personnel vetting process to reduce the time to bring new hires onboard, have more mobility, and ensure they're trusted through more nimble policy making, vetting tailored to mission needs, aligned security, suitability, and credentialing, reduced number of investigative tiers, and expanding the spectrum of investigative methods.

Visit the course Resources to access a job aid summarizing the key principles of each.

Review Activity 7

Which of the following best describes continuous vetting?

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

- ○ Periodic reinvestigations of an individual's background
- ○ Early investigations into an individual's background to determine eligibility for hire
- ○ Ongoing investigations only into individuals that pose a threat to national security
- ○ A near real-time review of an individual’s background at any time

Conclusion

Lesson Summary

You have completed the *Overview of Personnel Security* lesson. You should now be able to:

- Identify the primary components of the Personnel Security Program (PSP).
- Identify the key Executive Orders, policies, regulations, and guidelines that influence the personnel security methodology.
- Define the Trusted Workforce (TW) 2.0 framework and identify its key improvements in the reform of the personnel security process and establishment of a single vetting system.
- Identify continuous evaluation (CE) and continuous vetting (CV) requirements.

Lesson 3: Position Designation

Introduction

Lesson Objective

This lesson will discuss the Position Designation System, designation categories, and the Position Designation Tool.

Here is the lesson objective.

- Identify how the Position Designation System (PDS) determines the appropriate investigation, national security eligibility, and the level of access required for the corresponding position designation.

The Position Designation System

Overview of the PDS

As security professionals, you may hear people talk about their clearances. But these days we talk in terms of national security eligibility and the level of access that corresponds to their position designation. Position designations correlate to the potentially adverse impact on national security a position may have.

The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage to the efficiency, or integrity of, the service by misconduct of an incumbent of a position. This assessment also determines if a position's duties and responsibilities present the potential for position incumbents to bring about a material adverse effect on the national security, and the degree of that potential effect, which establishes the sensitivity level of a position. The results of this assessment determine what level of investigation should be conducted for that specific position. The position designation process ensures a systematic, dependable, and uniform way of making position risk and sensitivity designations in accordance with Parts 1400 and 731 of Title 5 of the Code of Federal Regulations (CFR). The PDS and associated Position Designation Tool (PDT) issued by the Executive Agents and hosted by the Defense Counterintelligence and Security Agency (DCSA) provide a method for departments and agencies to designate risk and sensitivity for all positions, including military service members, federal civilian employees, and contractors.

To determine the proper designation of a position and its required corresponding level of investigation, the position description, and any other necessary supplemental information, such as human resources or management and security office input, must be carefully evaluated to assess the nature of the position as it relates to the potential material adverse impact to the national security, and its impact on the efficiency or integrity of the service.

Definition of Access

As we discuss position designation it is important to understand the meaning of access. “Access” is the ability and opportunity to gain knowledge of classified information. This involves seeing, hearing, or touching classified information, material, or equipment.

The holder of information always controls access to the information or material. Therefore, the holder of the classified national security information has the responsibility to determine if the person seeking access has appropriate national security eligibility, a signed Standard Form 312 (SF-312), and a valid need-to-know for the information to carry out their official duties. Component and local organization procedures provide guidance on how to verify national security eligibility and need-to-know.

Types of Access

Not just anyone can access classified information. There are two basic types of authorizations for granting access depending on whether you are a U.S. citizen or a non-U.S. citizen.

If an individual is a U.S. citizen, that individual may receive a national security eligibility, or trust, determination. As noted previously, there are three levels of classified information: Top Secret, Secret, and Confidential. The degree of damage to national security that could result from its unauthorized disclosure determines which classification applies.

If an individual is not a U.S. citizen, that individual may receive a Limited Access Authorization (LAA). These two authorizations may be granted to civilian, military, and contractor personnel; however, their requirements for access will vary.

Designation Categories

Civilian Designation Categories

Civilian personnel designation requirements vary based on how the position is categorized. The Office of Personnel Management (OPM) defines the civilian position sensitivity levels as special-sensitive, critical-sensitive, non-critical sensitive, and non-sensitive. In addition to the four position levels, there is also a mixed-civilian designation.

Special-Sensitive

Special-sensitive national security positions are civilian national security positions that may potentially cause inestimable damage to the national security or adverse impact to the efficiency of the Department of Defense (DOD) or military services.

Critical-Sensitive

Critical-sensitive positions are civilian national security positions that have the potential to cause exceptionally grave damage to the nation’s security. Critical-sensitive positions include, but are not limited to:

- Positions requiring eligibility for access to Top Secret or Department of Energy (DOE) “Q” level classified information
- Positions involving development or approval of war plans, major or special operations of war, or critical and extremely important items of war
- National security policy-making or policy-determining positions, the duties of which have the potential to cause exceptionally grave damage to the national security
- Positions involving investigative duties, including handling of counterintelligence (CI) investigations or background investigations, the nature of which has the potential to cause exceptionally grave damage to the national security.

Non-Critical Sensitive

Non-critical sensitive positions can cause significant damage to national security. Non-critical sensitive positions include:

- Positions requiring eligibility for access to Secret, Confidential, or DOE "L" level information
- Positions not requiring eligibility for access to classified information, but having potential to cause significant or serious damage; positions requiring access to automated systems that contain military active duty, guard, or reservists’ personally identifiable information (PII)
- Positions designated by the DOD Component head

Non-Sensitive

If a position does not meet the criteria for any of the other position sensitivity levels, it is designated non-sensitive. These positions pose no potentially adverse effects on national security. Non-sensitive positions do not require access to classified information or performance of national security sensitive duties.

Mixed-Civilian

A mixed-civilian designation is a position involving job duties with different levels of impact on national security. Mixed duties involve any level of sensitive and/or non-sensitive or critical-sensitive and/or non-critical sensitive duties. When there is a mix of duties, the highest level of duty determines the sensitivity. The designation of sensitive positions meets the stated criteria for a specific security designation and is necessary to meet mission requirements.

Military/Contractor

Military and contractor personnel have designations distinct from civilian employees. Both military and contractor personnel are granted eligibility to access classified information and perform national security sensitive duties comparable to civilians. Military occupational specialties or billets have specific eligibility and access requirements. For contractors and industry personnel the requirements for eligibility and access are included in the Department of Defense (DD) Form 254 "Contract Security Classification Specification."

Visit the course Resources to access a job aid summarizing the designation categories.

Other Designations

Only U.S. citizens are eligible for access to classified information. However, when compelling reasons exist, non-U.S. citizens who require classified access to perform official duties can be granted an LAA at no higher than the Secret level.

Special Types of Information

There are some special requirements for access to information related to programs that impose access controls beyond those normally provided for Confidential, Secret, or Top Secret information. Special programs provide an additional layer of security for some of our nation's most sensitive assets. When an individual's work involves access to such information, they require a more extensive national security background investigation and adjudication. Special programs cover a variety of areas, including: Presidential support activities, special access programs, the North Atlantic Treaty Organization (NATO), the Nuclear Personnel Reliability Program (Nuclear PRP), Sensitive Compartmented Information (SCI), Nuclear Command and Control – Extremely Sensitive Information (NC2-ESI), and Chemical Personnel Reliability Program (Chemical PRP).

Review Activity 1

Lea is an Analyst who works at a DOD agency. She is a civilian who works on projects that have varying levels of impact on national security. One of her projects involves reviewing war plans that require access to Top Secret information. Which of the following categories describes Lea's civilian position?

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

- ○ Non-critical sensitive
- ○ Critical-sensitive
- ○ Special-sensitive

Review Activity 2

Frank is a member of the Canadian Air Force. He is on a temporary assignment working at a DOD agency and needs access to classified information. Frank has unusual expertise and knowledge for a

position that a U.S. citizen does not have. To be eligible to do the job, Frank receives which of the following?

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

- ○ Access
- ○ National Security eligibility
- ○ Limited Access Authorization

Position Designation Tool

PDT Overview

The Position Designation Tool (PDT) is used to guide personnel through the Position Designation System (PDS) process. The National Background Investigation System (NBIS) provides the PDT as an automated means for agencies to complete proper validation of covered positions.

The requirement for designation of all covered positions is outlined in 5 CFR Part 731. Additional requirements for designating National Security Positions are outlined in 5 CFR Part 1400. The regulations provide the standard for agencies to assess duties of covered positions for their potential risk to the integrity of public trust and degree of potential damage to national security. The assessed combination of a position's national security and public trust duties determine the appropriate level of investigation for a position.

PDT Purpose

The PDT provides agencies with a methodical and uniform system to accurately evaluate covered positions. To help government employees assess the risk and sensitivity level for a covered position, the requirements outlined in 5 CFR Parts 731 and 1400 are displayed in the application in accordance with OPM and the Office of the Director of National Intelligence (ODNI).

The PDT allows users to choose relevant responsibilities and duties for the position and assess the level of risk and potential damage associated with those duties. After a PDT user has entered all required information about the position, a final summary page outlines the sensitivity and risk level for the position, as well as the required investigation and standard form type for a candidate to fill that position.

Conclusion

Lesson Summary

You have completed the Position Designation lesson. You should now be able to:

- Identify how the Position Designation System (PDS) determines the appropriate investigation, national security eligibility, and the level of access required for the corresponding position designation.

Lesson 4: Investigations

Introduction

Lesson Objectives

This lesson will discuss the investigation process, including the investigative tiers and the five personnel vetting scenarios.

Here are the lesson objectives.

- Apply the investigative process and investigative tiers based on adjudicative attributes in given scenarios.
- Using situational examples, distinguish the five personnel vetting scenarios based upon the mission need, relevant circumstances, duties and responsibilities of the position, and the management of human risk.

The Investigations Process

Investigations Process Overview

In the interest of safeguarding the welfare of the American people, it is required that all persons privileged to be employed in the departments and agencies of the United States government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States. Executive Order 10450 requires a background investigation to be conducted on each civilian officer or employee in any department or agency of the government. The scope of the investigation will vary, depending on the nature of the position and degree of harm that could be caused by the individual in that position. Requirements to be investigated for the purpose of a suitability determination apply whether or not the position requires a national security eligibility, or access to classified national security information.

General Background Investigative Process

The general process for background investigations involves six steps. The first step is position designation, followed by completion of the Standard Form, often referred to as Personnel Security or Personnel Vetting Questionnaire, and its submission. Following submission of the Standard Form is the investigation. Based on the results of the investigation, an adjudicative, or trust, determination is made. Finally, the individual enters Continuous Vetting (CV).

Investigative Standards

Three-Tier Investigative Model

The Trusted Workforce (TW) 2.0, Federal Personnel Vetting Investigative Standards are used to determine the scope of the background investigation.

The model has three tiers.

- The Low Tier (LT) includes positions designated as non-sensitive, low risk, and is the minimum investigative tier for eligibility for physical and/or logical access or credentialing determinations. Homeland Security Presidential Directive 12 (HSPD-12) Credentialing is included in this tier.
- The Moderate Tier (MT) includes positions designated as non-sensitive moderate-risk public trust and/or non-critical sensitive moderate-risk public trust. For non-critical sensitive positions, the level of investigation can be used to grant access to classified information at the Confidential or Secret level, or "L" access.
- The High Tier (HT) includes positions designated as non-sensitive high-risk public trust and/or critical-sensitive high-risk public trust or special-sensitive high-risk public trust. For critical- or special-sensitive positions, the level of investigation can be used to grant access to classified information at the Top Secret level, access to Sensitive Compartmented Information or SCI, or "Q" access.

The investigative tiers are appropriately aligned to support trust determinations for suitability, fitness, national security, and/or credentialing, as appropriate, to the designations at each level of risk, and to permit mobility to the greatest extent possible. The investigation for each tier builds upon the lower tiers, with the coverage and complexity of each tier corresponding with the position designation for which the individual is being vetted.

Visit the course Resources to access a job aid summarizing the investigative tiers.

Information Types

The three-tier investigative model uses the following information types: database checks, written inquiries, interviews, and records. For instance, the LT investigation consists of several elements, including database and local agency checks as well as written inquiries. These information types align with the investigative standards and gather the relevant information needed to assess the characteristics of a trusted person that will protect people, property, information, and mission.

Crosswalk

This new three-tier model replaces the previous five-tier model. Tier 1 of the five-tier model becomes LT. Tiers 2 and 3 become MT. Tiers 4 and 5 become HT.

Previous Tier	Position Designations by Tier
Tier 1	Low Risk Non-Sensitive Physical and Logical Access (HSPD-12) Credentialling
Tier 2	Moderate Risk Public Trust
Tier 3	Non-critical sensitive Secret/Confidential "L" Access
Tier 4	High Risk Public Trust
Tier 5	Critical-Sensitive Special-Sensitive Top Secret Sensitive Compartmented Information "Q" Access

TW 2.0 Tier	Position Designations by Tier
Low Tier	Non-Sensitive/Low Risk Physical and Logical Access (HSPD-12) Credentialling
Moderate Tier	Non-Sensitive/Moderate-Risk Public Trust Non-Critical Sensitive/Moderate-Risk Public Trust Secret/Confidential "L" Access
High Tier	Non-Sensitive/High-Risk Public Trust Critical-Sensitive/High-Risk Public Trust Special-Sensitive/High-Risk Public Trust Top Secret Sensitive Compartmented Information "Q" Access

Review Activity 1

For each personnel file, determine the appropriate investigative tier. Check your answers in the Answer Key at the end of this Student Guide.

Question 1 of 4

Subject: Isabel Armstrong

Role: Program Manager

- Non-critical sensitive position
- Requires access to Secret level classified information

- ○ Low Tier (LT)
- ○ Moderate Tier (MT)
- ○ High Tier (HT)

Question 2 of 4

Subject: Alex Chang

Role: Human Resources Specialist

- Non-sensitive/Low risk
- Requires HSPD-12 Credentialing

- ○ Low Tier (LT)
- ○ Moderate Tier (MT)
- ○ High Tier (HT)

Question 3 of 4

Subject: Christopher Ruiz

Role: Navy Engineer

- Special-sensitive position
- Requires access to Sensitive Compartmented Information (SCI)

- ○ Low Tier (LT)
- ○ Moderate Tier (MT)
- ○ High Tier (HT)

Question 4 of 4

Subject: Zakiya Thomas

Role: Senior Intelligence Specialist

- Critical-sensitive position
- Requires access to Top Secret level classified information

- ○ Low Tier (LT)
- ○ Moderate Tier (MT)
- ○ High Tier (HT)

The Five Vetting Scenarios

Five Vetting Scenarios Overview

The new Federal Personnel Vetting Investigative Standards map the investigative requirements for five personnel vetting scenarios based on mission needs, position designation, and an individual's relevant personnel history information. The scenarios include initial vetting, continuous vetting (CV), upgrades, transfer of trust, and re-establishment of trust.

Visit the course Resources to access a job aid summarizing the vetting scenarios.

Now let's take a closer look at each vetting scenario.

Initial Vetting Overview

Initial Vetting establishes trust. Let's look at what occurs during initial vetting.

First, departments and agencies determine the individual's appropriate position designation and the investigative tier required. They then gather the necessary documentation via the corresponding Standard Form from the individual and submit the investigative request to the investigative service provider (ISP). ISPs conduct the investigation in accordance with the Federal Personnel Vetting Investigative Standards requirements.

For a rapid vetting process, ISPs conduct the required high-yield automated record checks, which then allows departments and agencies to make preliminary, commonly known as temporary or interim, eligibility determinations. ISPs must report information identified as "substantial" or "major" to the requesting department or agency to decide if an immediate action is required prior to conducting additional investigative activity.

CV Overview

CV maintains trust. CV is performed to maintain the federal government's confidence that the individual will continue to protect people, property, information, and mission.

It is imperative that departments and agencies proactively and continuously assess their trusted workforce to promote early detection of potential problems, reduce risk, and address concerning behaviors and perceived vulnerabilities as they emerge.

CV occurs on an on-going basis, including automated data source checks and investigative activities at intervals based on the investigative tier.

CV Purpose

CV enables departments and agencies to address potential risks in a more deliberate manner and in near real-time by integrating information categories and data sources tailored to the individual's personal circumstances and the potential risk presented by the duties and responsibilities of the position.

The level of CV will vary in terms of required coverage, periodicity, and triggered events. This vetting scenario must consider the minimum conditions, information categories, and frequency of personnel vetting conducted on an individual to mitigate risk and ensure trust.

This enables departments and agencies the flexibility to customize the level of personnel vetting to the mission risk and supports the mobility of the trusted workforce. Periodic reinvestigations have been replaced completely with CV. However, periodic completion of investigation forms such as Standard Form 85 (SF-85), SF-85P, and SF-86 still occur at five-year intervals, and additional investigations may be triggered by the results of CV.

Upgrades Overview

Upgrades occur when a subject has undergone an initial trust determination, been enrolled in compliant CV, and moves to a new position requiring a higher-level investigation within or on behalf of the same department or agency. Departments and agencies should only request the investigative items needed to fully meet the coverage requirements at the new investigative tier. The request must include any relevant self-reported or agency-specific information. When there is a developed issue information, the ISP will expand the investigation to address any relevant information. The coverage requirements for each information category generally expand at higher tiers.

Transfer of Trust Overview

The Transfer of Trust vetting scenario is a process for ensuring that investigative information is available and accessible, as appropriate, when individuals transfer across departments or agencies and across roles. This vetting scenario is commonly referred to as reciprocity. ISPs should not conduct duplicative investigations and should alert departments or agencies if an investigation is in process or has recently closed. Transfer of trust requires transparency in ISPs reporting and information-sharing to prevent redundant personnel vetting actions on trusted insiders.

Re-establishment of Trust Overview

Re-establishment of Trust is the process used for an individual who stops performing work for or on behalf of the federal government, or is no longer in a position that subjects them to CV, for a period of time. If the break in service is less than 36 months, the gaining department or agency will need to

determine whether to accept the previous investigation or CV activities. Breaks in service greater than 36 months will require the individual to go through initial vetting.

The degree of personnel vetting to re-establish trust should be personalized to address the new position designation; the length of time the individual was not affiliated with the government; the individual's prior personnel vetting record, including known issue information, exceptions, and enrollment in CV; any previously known but unadjudicated information reflected in the individual's federal personnel vetting record; and any new issue information that requires review.

Re-establishment of Trust Considerations

Based on the assessment of the individual's circumstances, the department or agency may request the ISP conduct additional personnel vetting prior to making the decision to re-establish trust. New personnel vetting should be limited to those information categories and data sources necessary to re-establish the baseline of trust according to the position designation. The ISP must immediately refer any new issue information developed to the department or agency for consideration in re-establishing trust and whether to request additional personnel vetting.

If the new position requires a higher investigative tier than the tier to which the individual was previously vetted, the gaining department or agency must request the ISP conduct the additional investigative requirements for the higher tier.

Review Activity 2

Question 1 of 3. Dave is a program manager for a project for the Office of Naval Research. The project is coming to an end. To support mission needs, Dave is moved on to manage a project for the Naval Education and Training Command which is the same sensitivity level and requires the same level of access.

Which personnel vetting scenario is Dave subject to?

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

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Question 2 of 3. Aria is an Intelligence Specialist for the National Security Agency (NSA). She has already undergone an initial trust determination and been enrolled in CV for her current position, which is a non-critical sensitive position with access to Secret level classified information. Aria

accepts a new position as a Senior Intelligence Specialist within the NSA. This new position, however, is critical-sensitive and requires access to Top Secret level information.

Which personnel vetting scenario is Aria subject to?

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

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Question 3 of 3. Van is a software engineer that left their DOD position to work for a private company. After one year in the private sector, Van returns to the DOD at the same position designation and sensitivity level

Which personnel vetting scenario is Dave subject to?

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

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Conclusion

Lesson Summary

You have completed the *Investigations* lesson. You should now be able to:

- Apply the investigative process and investigative tiers based on adjudicative attributes in given scenarios.
- Using situational examples, distinguish the five personnel vetting scenarios based upon the mission need, relevant circumstances, duties and responsibilities of the position, and the management of human risk.

Lesson 5: Adjudications

Introduction

Lesson Objectives

This lesson will discuss the adjudications phase, including the whole person concept, types of adjudications, due process, and recording final determinations.

Here are the lesson objectives.

- Identify the guidelines and factors of the adjudicative methodology.
- Apply the key elements and considerations for each type of adjudication through given scenarios.
- Apply the process for handling unfavorable adjudication determinations to various personnel candidates' circumstances and data points.
- Identify the key elements of reconsiderations, reinstatements, and the recording of final determinations.

The Whole-Person Concept and Adjudicative Methodology

Adjudication Overview

Adjudication is the process of making a trust determination. The adjudicative process begins once a personnel security investigation is completed by the investigative service provider (ISP) and sent to the Consolidated Adjudication Services (CAS) for a national security eligibility trust determination. The adjudication serves as the key component in ensuring that an applicant does not pose an unacceptable risk to DOD assets.

The Whole-Person Concept

The adjudicative process is an examination of a sufficient period and a careful weighing of a number of variables of an individual's life to make an affirmative determination that the individual is an acceptable security risk. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a national security eligibility determination. This is known as the whole-person concept. When making national security eligibility trust determinations, adjudicators must use the whole-person concept. Adjudicators must consider the uniqueness of each case, which must be judged on its own merits, based on the disqualifying and mitigating conditions.

Nine Adjudicative Factors

Adjudicators must receive formal training to ensure consistency and fairness. To sort through all the information received about an applicant, adjudicators use several tools. Adjudicators use nine

adjudicative factors to help evaluate both past and present, and the favorable and unfavorable information about a subject's conduct. These factors include the nature, extent, and seriousness of the conduct; the circumstances surrounding the conduct, to include knowledgeable participation; the frequency and recency of the conduct; the individual's age and maturity at the time of the conduct; the extent to which participation is voluntary; the presence or absence of rehabilitation and other permanent behavioral changes; the motivation for the conduct; the potential for pressure, coercion, exploitation, or duress; and the likelihood of continuation or recurrence.

Review Activity 1

Which of the following best describes what an adjudicator must do when making trust determinations?

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

- ○ Collect unfavorable information from a person's past.
- ○ Review a written narrative from the subject detailing their lived experience.
- ○ Review an individual's past employment history.
- ○ Examine all available and reliable information about the person, past and present, favorable and unfavorable.

Adjudicative Process Framework

Order of Operations

Adjudicators use the adjudicative process framework to assess the potential risk presented by individuals to determine if the risk can be managed or mitigated, and to make a trust determination. Trust determinations are made in the following sequence known as the order of operations. First, an agency must determine if an individual has the character and conduct to carry out the duties and responsibilities of a federal job by conducting either a Suitability or Fitness trust determination. Once a Suitability or Fitness trust determination is made, if appropriate, an agency can conduct a national security trust determination, which includes considerations for access to classified information. Next, an agency can conduct a credentialling trust determination if an individual requires physical access to federal-controlled facilities or information systems. Note that each of these domains have a distinct purpose, requirements, and adjudicative criteria. It is also possible for an individual to receive a favorable trust determination for one domain but an unfavorable determination for another. For instance, an individual could be determined suitable for federal employment but not eligible for access to classified information.

Let's take a closer look at the distinctions between suitability, fitness, and credentialing trust determinations. We will cover national security trust determinations later in this lesson.

Suitability Adjudication

The Office of Personnel Management (OPM) establishes policy and procedures for Suitability and Fitness (as requested) trust determinations. Suitability refers to identifiable character traits and conduct that indicate a candidate is likely to carry out the duties of a federal job with integrity,

efficiency, and effectiveness. This process examines investigative results in the context of OPM's eight suitability factors and seven additional considerations. For more information see the *Introduction to Suitability Adjudications for the DOD* course.

Fitness Adjudication

OPM also establishes policy and procedures for Fitness trust determinations. Fitness determinations follow much of the same program guidance as suitability and are applied to excepted service positions, which cannot be converted to the competitive service, or otherwise are not subject to suitability; DOD contractor positions; and Non-appropriated Fund (NAF) positions.

HSPD-12 Adjudication (Credentialing)

Homeland Security Presidential Directive 12 (HSPD-12) trust determinations determine who may be issued credentials for physical access to federal-controlled facilities or federal controlled information systems. Within the DOD this identity credential is known as the Common Access Card (CAC) and is a trusted credential for use across the federal government. The primary purpose of HSPD-12 vetting is to ensure that individuals are not known or suspected terrorists, do not provide an avenue for terrorism, and do not pose an unacceptable risk to employees or DOD assets. During the review process of the investigation, adjudicators use 13 credentialing standards. For more information see the *Introduction to DOD HSPD-12 CAC Credentialing* course.

Review Activity 2

Question 1 of 2. Review the scenario and determine the appropriate trust determination.

Logan was hired as a contractor for a DOD agency. What trust determination is used to determine whether Logan has the character or conduct necessary for the position?

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

- ○ Suitability adjudication
- ○ Fitness adjudication
- ○ HSPD-12 adjudication

Question 2 of 2. Review the scenario and determine the appropriate trust determination.

Tanya was hired as an analyst for a DOD agency. She requires logical access to federal controlled information systems. What trust determination is used to issue credentials for logical access?

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

- ○ Suitability adjudication
- ○ Fitness adjudication
- ○ HSPD-12 adjudication

National Security Adjudication

National Security Adjudication Overview

National security adjudication is a PV process which seeks reasonable assurance that persons granted access to classified information, or hold sensitive positions, are loyal, trustworthy, and reliable. When making national security eligibility, trust determinations, adjudicators use 13 National Security adjudicative guidelines and nine factors found in Security Executive Agent Directive 4 (SEAD 4). They use these guidelines and factors when evaluating information, which may or may not be a security concern, to determine if a candidate is an acceptable risk to national security.

Let's take a brief look at the guidelines.

National Security Adjudicative Guidelines

Each of the 13 national security adjudicative guidelines in SEAD 4 identifies a potential security concern that may have an adverse impact on national security.

Some guidelines deal with cases in which a subject's allegiance to the U.S. may be in question including A. Allegiance to the United States, B. Foreign Influence, and C. Foreign Preference.

There are guidelines that deal with cases in which the subject's character, or their reliability, trustworthiness, and ability to protect classified information enter into question including D. Sexual Behavior, E. Personal Conduct, and F. Financial Considerations.

Other guidelines deal with health matters that might influence an individual's ability to protect classified information including G. Alcohol Consumption, H. Drug Involvement and Substance Misuse, and I. Psychological Conditions.

Finally, some guidelines cover illegal and other noncompliant behaviors including J. Criminal Conduct, K. Handling Protected Information, L. Outside Activities, and M. Use of Information Technology.

Each specific guideline carries with it three components: the concern, conditions that could raise a security concern and may be disqualifying, and conditions that could mitigate security concerns.

Review Activity 3

Review the scenario and determine the appropriate national security adjudicative guideline.

Lindsay is a newly assigned civilian employee who requires Top Secret eligibility. During a background investigation, an investigator interviewed Lindsay and learned that, when she was in college, she was the secretary of the New Free America Liberation Coalition. This group's goal is to overthrow the U.S. government and establish a worker state. This group seeks to achieve its goal through any means, including violence.

While Lindsay supported the concept of a worker state, she thought it would come about through the election process. When she learned the full extent of the group's goals, she left the organization.

What adjudicative guideline applies to this scenario?

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

- ○ A. Allegiance to the United States
- ○ F. Financial considerations
- ○ I. Psychological Conditions
- ○ K. Handling Protected Information

Review Activity 4

Review the scenario and determine the appropriate national security adjudicative guideline.

John was born in the United States to British citizens who were legally residing and working in the United States at the time of his birth. He acquired British citizenship through his parents and has a current British passport. He is applying for a position in the U.S. government that requires Top Secret eligibility. As required, he disclosed his foreign citizenship and passport on his security form.

During the interview portion of his investigation, John disclosed that even though he was born in the United States, he holds British citizenship through his parents and maintains a British passport. He advised he only uses his U.S. passport when traveling to and from the United States. He also stated that he does not exercise any rights, privileges, or obligations associated with his foreign citizenship and does not hold any foreign financial or business interests.

What adjudicative guideline applies to this scenario?

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

- ○ C. Foreign Preference
- ○ F. Financial considerations
- ○ I. Psychological Conditions
- ○ K. Handling Protected Information

Due Process

Due Process for All Overview

Before an unfavorable national security eligibility determination is made there are several requirements including specific items provided to the individual, the opportunity for the individual to appeal the determination, and the government's decision regarding the appeal. This is referred to as due process. Due process is an established administrative process designed to ensure the fair and impartial adjudication of facts and circumstances when an unfavorable national security eligibility is being considered. The process is offered to individuals before a final unfavorable determination is made.

Let's take a closer look at the specific requirements of due process.

Provisions to Individual

According to the DOD Manual 5200.02, Procedures for the DOD Personnel Security Program, the minimum due process requirements indicate the individual must be provided a letter of denial (LOD) or letter of revocation (LOR). The LOD or LOR must include a comprehensive and detailed written explanation of the basis for the unfavorable determination. In particular, it must include each security concern, the applicable adjudicative guideline or guidelines related to each concern, and an explanation of the kinds and types of information individuals can provide to support their appeal. The individual must acknowledge the receipt of the LOD or LOR and indicate in writing if they will submit an appeal. If the individual refuses to acknowledge receipt, the security professional will make a written record of the refusal and submit it to the adjudication facility.

The individual must also be provided with a written notice of reasons for the determination to include the determination of each adjudicative guideline that was provided to the individual in the statement of reasons (SOR) that accompanied the notification of intent (NOI) to deny or revoke national security eligibility. The individual must be informed of their right to be represented by counsel or other representative at their own expense. They also must be allowed to request the documents, records, and reports from which the unfavorable national security determination was made. Individuals must be provided a reasonable opportunity to reply in writing and to request review of the unfavorable determination. Individuals must also be provided with written notice of the right to appeal unfavorable determinations to a high-level panel.

Opportunity to Appeal

For the appeal, the individual must indicate in writing if they are going to submit an appeal. If the individual refuses to acknowledge receipt or indicate whether an appeal will be submitted, the security professional will make a written record of the refusal and submit it to the adjudication facility. The individual must be provided an opportunity to appear in person and present relevant witnesses, documents, materials, and information.

Decision on Appeal

On an appeal, the individual must be provided a written decision.

Due Process for Civilian Employees and Military Members Overview

There are also specific procedures for due process for civilian employees and military members that must occur before an unfavorable national security eligibility determination can be made including specific items provided to the individual, the opportunity for the individual to appeal the determination, and the government's decision regarding the appeal.

Let's take a closer look at each.

Provisions to Individual (Civilian and Military)

The civilian employee or military member must be provided with a letter of intent (LOI) to deny or revoke eligibility, and a written SOR stating the basis for the proposed unfavorable national security eligibility determination. Similar to the general due process, the SOR must be comprehensive and

detailed including providing an explanation of each security concern, the specific facts that trigger each security concern, the applicable adjudicative guideline or guidelines for each concern, and the disqualifying and mitigating conditions for each adjudicative guideline cited. The civilian employee or military member must be afforded an opportunity to reply to the LOI and SOR. The reply must be in writing to the adjudication facility. In addition, the adjudication facility will provide the individual with a written LOD or LOR via the appropriate Component or command security office. The LOD or LOR must state the final determination of each adjudicative guideline that was provided to the individual in the SOR, what was mitigated or unmitigated, and a reason or reasons for denying or revoking national security eligibility.

Opportunity to Appeal (Civilian and Military)

The civilian employee or military member must be afforded an opportunity to appeal the LOD or LOR. Within 10 calendar days of receipt of the LOD or LOR, the individual will sign and return the notice of intent to appeal (NOIA) to the adjudication facility via their security office. The individual must state whether they intend to appeal, and if so, whether they request a personal appearance or if they will appeal in writing.

Decision on Appeal (Civilian and Military)

The DOD Component will review the adjudicative file and any appeal materials and render a final decision. The civilian employee or military member must be provided with a final written decision by the DOD Component. If the DOD Component determines that more information is needed to render a final determination, such as an updated credit bureau report or information from the command, that information must be provided to the individual. The individual must then be provided a reasonable period of time to offer any rebuttal to this information.

Review Activity 5

Shannon is a civilian employee for a DOD agency. She is transferring to a position that is designated as higher risk and requires greater eligibility access than her current position, so she is being investigated for the upgrade. During the interview portion of her personnel security investigation, Shannon told the investigators that she purposefully omitted information about her involvement in a drug related crime.

According to due process for civilian employees, what must occur before an unfavorable national security eligibility determination is made?

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

- ☐ Shannon must be provided a Letter of Intent (LOI).
- ☐ Shannon must be provided a Statement of Reasons (SOR).
- ☐ The agency must audit the personnel security investigation.
- ☐ Shannon must be provided an opportunity to appeal.
- ☐ The ISP must reinvestigate Shannon within 60 days.

Review Activity 6

If the adjudication facility provides Shannon with a Letter of Denial (LOD) or Letter of Revocation (LOR), what will be stated?

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

- ☐ Final determination of each adjudicative guideline that was provided in the Statement of Reasons (SOR)
- ☐ What was mitigated or unmitigated
- ☐ Steps to follow to appeal the decision
- ☐ Reason(s) for denying or revoking national security eligibility

Recording Final Determinations, Reconsideration, and Reinstatement

Final Determinations, Reconsideration, and Reinstatement Overview

After due process for an unfavorable national security eligibility, the DOD Component will record final determinations. In some circumstances individuals may be reconsidered and reinstated.

Let's take a brief look at the processes and requirements for recording final determinations, reconsideration, and reinstatement.

Recording Final Determinations

The DOD Component provides electronic copies of all final decisions to the adjudication facility that made the initial unfavorable determination. The adjudication facility updates the system of record within two calendar days to reflect current eligibility and attaches the DOD Component decision to the individuals' adjudicative records.

Reconsideration

The DOD Component may request reconsideration of unfavorable national security determinations for individuals within their agency, department, or command to address specific mission needs. Note that individuals are eligible after one year following the denial or revocation. Request for reconsideration must be made to the adjudication facility from the security office or offices and must meet an operational need of the DOD Component. Reconsideration cases will not be resubmitted or reassessed solely based on an individual's personal desire to acquire eligibility. Reconsideration is not a personal right or entitlement.

Security offices must include evidence that the issues which caused the denial or revocation have been resolved. Security offices are responsible for ensuring DOD Component requests for reconsideration are complete. Once security offices submit their DOD Components' request for reconsideration, no supplemental information will be accepted or considered unless requested by the adjudication facility. Note that a DOD Component's request for reconsideration does not reopen or otherwise affect the denial or revocation decision. When reconsidered, individuals will be submitted for a new investigation.

Reinstatement

For a DOD civilian employee to be reinstated, restored to duty, or reemployed in a sensitive or national security position in the DOD, it must be clearly consistent with the interests of national security. Only the employee's DOD Component head can reinstate the employee. Also, the finding must be made part of the employee's personnel security record.

Review Activity 7

At which point is an individual eligible for reconsideration following an unfavorable national security determination?

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

- ○ Immediately after the denial or revocation
- ○ 30 days following the denial or revocation
- ○ 1 year following the denial or revocation
- ○ 5 years following the denial or revocation

Review Activity 8

Which of the following is true regarding reinstating a DOD civilian after an unfavorable national security determination?

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

- ☐ Reinstatement must be in the interest of national security.
- ☐ The security office makes the final determination on reinstatement.
- ☐ Reinstatement prevents the need for a new investigation.
- ☐ The DOD Component head can reinstate the employee.
- ☐ The employee's supervisor may temporarily reinstate them.

Conclusion

Lesson Summary

You have completed the *Adjudications* lesson. You should now be able to:

- Identify the guidelines and factors of the adjudicative methodology.
- Apply the key elements and considerations for each type of adjudication through given scenarios.
- Apply the process for handling unfavorable adjudication determinations to various personnel candidates' circumstances and data points.
- Identify the key elements of reconsiderations, reinstatements, and the recording of final determinations.

Lesson 6: Security Responsibilities and Duties

Introduction

Lesson Objectives

This lesson will examine security responsibilities and duties, including the security professional's education, training, and briefings; Security Executive Agent Directive 3 (SEAD 3) reporting requirements; and the responsibilities of various security levels.

Here are the lesson objectives.

- Identify the security professional's responsibilities, including education and training requirements.
- Through situational examples, classify the duties and reporting requirements for all covered individuals who have access to classified information or hold a sensitive position.

Security Professional's Responsibilities Overview

Supervisors, managers, and security professionals play a critical role in assuring the success of the PSP. As discussed, the goal of CV is timely detection and reporting of potential issue information. Security personnel are informed of their personnel security responsibilities and provided guidance on indications of potential personnel security concerns and procedures to follow. This allows them to report these concerns in a timely manner. In particular, Personnel Security Programs include training and continuous education on reportable behaviors, procedures for immediate reporting of potentially derogatory and adverse information through appropriate channels to the appropriate adjudication facility, and outreach to inform personnel of their reporting responsibilities, and programs to address behaviors that may affect their continued eligibility for access to classified information or assignment to a sensitive position.

Security Professional's Education, Training, and Briefings

Education and Training Programs

Department of Defense (DOD) security professionals and other personnel performing security duties are required to complete security education and training programs on the procedures necessary to protect information and on the personnel security process. Training topics include information systems and intelligence threat briefings. The Center for Development of Security Excellence (CDSE) website includes personnel security courses, job aids, reference guides, webinars addressing the security eligibility process, and various "security shorts."

Briefings Overview

One important responsibility of the security office is to conduct briefings. Security briefings take place to provide important security information to individuals who perform work in a secure environment. Security professionals take part in initial, refresher, insider threat, and termination briefings.

Let's take a closer look at each type of briefing.

Initial Briefing

Security professionals give an initial security briefing to all personnel with national security eligibility before they gain access to classified information. This briefing must comply with the requirements of Executive Order (E.O.) 12968; and the Department of Defense Manual (DODM) 5200.01, Volume 3. All individuals must complete the appropriate nondisclosure forms in accordance with Section 552 of Title 5, United States Code. If individuals decline to complete the nondisclosure forms, the DOD Component will withhold classified access and report the refusal to the adjudication facility. Note that DOD Components will maintain records of all initial briefings.

Refresher Briefing

Security professionals provide refresher briefings annually, as well as when there are changes in security regulations, policies, or procedures. Personnel with national security eligibility will receive annual refresher security training in accordance with DODM 5200.01. Security education should be on a continuing basis, taking into account each person's duties, experience, and past conduct involving the protection of classified or sensitive information. Note that DOD Components will maintain records of all refresher training conducted.

Insider Threat Briefing

Insider threat awareness is incorporated in security training in accordance with Department of Defense Directive (DODD) 5240.06 and Department of Defense Instruction (DODI) 5240.26.

Termination Briefing

Security professionals provide termination briefings to service members, federal civilian employees, and contract employees when employment terminates, national security eligibility is withdrawn, or another absence excludes the individual from CV authorizations. These briefings are required by DODM 5200.01. For individuals with Sensitive Compartmented Information (SCI) access, they must also complete the Security Debriefing Acknowledgement and Debrief blocks located on the reverse side of the DD Form 4414, "Sensitive Compartmented Information Nondisclosure Agreement."

Review Activity 1

Which of the following security professional briefings are completed annually and when there are changes to policies or procedures?

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

- ○ Initial Briefing
- ○ Refresher Briefing
- ○ Insider Threat Briefing
- ○ Termination Briefing

SEAD 3 Reporting Requirements

SEAD 3 Reporting Requirements Overview

All individuals who have access to classified information or hold a sensitive position must follow strict reporting requirements. SEAD 3 outlines these requirements including reportable activities for all covered individuals; reportable actions by others; reporting requirements for individuals with access to Secret and Confidential information, "L" access, or holding a non-critical sensitive position; and reporting requirements for individuals with access to Top Secret information, "Q" access, or holding a critical- or special-sensitive position.

Let's take a closer look at each.

Reportable Activities

Reportable activities for all covered individuals include foreign travel and foreign contacts.

Foreign Travel

Covered individuals must submit an itinerary for unofficial foreign travel to their agency head or designee and they must receive approval prior to travel. Heads of agencies, or their designees, may disapprove an unofficial foreign travel request if it presents an unacceptable risk or if an individual's physical safety and security cannot be reasonably ensured.

Foreign Contacts

Unofficial contact involves contact with a known or suspected foreign intelligence entity. This includes continuing association with known foreign nationals that involve bonds of affection, personal obligation, intimate contact, or any contact with a foreign national that involves the exchange of personal information. In general, individuals are not required to report limited or casual public contact with foreign nationals. Note that heads of agencies, or their designees, may provide more specific guidance.

Reportable Actions by Others

To ensure the protection of classified information or other information specifically prohibited by law from disclosure, covered individuals must alert agency heads or designees to reportable activities of other covered individuals that may be of potential security or counterintelligence (CI) concern. These activities include:

- An unwillingness to comply with rules and regulations or to cooperate with security requirements
- Unexplained affluence or excessive debt
- Alcohol abuse
- Illegal use or misuse of drugs or drug activity
- Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified information
- Criminal conduct
- Any activity that raises doubts as to whether another covered individual's continued national security eligibility is clearly consistent with the interests of national security
- Misuse of U.S. government property or information systems

Individuals with Access to Secret and Confidential Information

Individuals with access to Secret and Confidential information, “L” access, or holding a non-critical sensitive position must also report:

- Foreign activities, including application for and receipt of foreign citizenship, or application for, possession of, or use of a foreign passport or identity card for travel
- Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information prohibited from disclosure
- Media contacts, other than for official purposes, where the media seeks access to classified information or other information prohibited from disclosure
- Arrests
- Bankruptcy or over 120 days delinquent on any debt
- Alcohol-and drug-related treatment

Individuals with Access to Top Secret Information

Individuals with access to Top Secret information, "Q" access, or holding a critical- or special-sensitive position must also report:

- Foreign activities, including direct involvement in foreign business, foreign bank accounts, ownership of foreign property, application for and receipt of foreign citizenship, application for, possession of, or use of a foreign passport or identity card for travel, voting in a foreign election, and adoption of non-U.S. citizen children
- Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information prohibited from disclosure
- Media contacts where the media seeks access to classified information or other information prohibited from disclosure
- Financial anomalies, including bankruptcy, garnishment, over 120 days delinquent on any debt, and any unusual gain of assets of $10,000 or greater such as an inheritance or winnings
- Arrests
- Foreign national roommates, which includes any foreign national who co-occupies a residence for over 30 days
- Cohabitants
- Marriage
- Alcohol- and drug-related treatment

Review Activity 2

Question 1 of 2. Danielle is a civilian employee at the DOD in a non-critical sensitive position. According to SEAD 3 reporting requirements, what activities is Danielle responsible for reporting based on her position?

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

- ☐ U.S. citizen roommates
- ☐ Unofficial media contacts
- ☐ Arrests
- ☐ Adoption of non-U.S. citizen children
- ☐ Alcohol- and drug-related treatment

Question 2 of 2. Sal is a military member of the DOD in a critical-sensitive position with access to Top Secret classified information. According to SEAD 3 reporting requirements, what activities is Sal responsible for reporting based on his position?

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

- ☐ U.S. citizen roommates
- ☐ Unofficial media contacts
- ☐ Arrests
- ☐ Adoption of non-U.S. citizen children
- ☐ Alcohol- and drug-related treatment

Review Activity 3

Ronald is a contractor at a DOD agency. He is in a moderate-risk public trust position.

True or False. Ronald must receive approval from his agency head for any unofficial foreign travel.

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

- ○ True
- ○ False

Security Professional's Responsibilities

Role-Specific Responsibilities Overview

There are role-specific security responsibilities for the Security Executive Agent (SecEA), heads of agencies, supervisors, security professionals, employees, and individuals.

Let's take a closer look at the responsibilities for each role.

SecEA

The SecEA is responsible for monitoring the effectiveness of reporting requirements, developing recommendations for new or modified requirements, overseeing agency compliance, and ensuring best practices are identified, shared, and implemented.

Heads of Agencies

Agency heads are responsible for:

- Developing agency reporting guidance and processes
- Automating and centralizing reporting
- Maintaining reported information

- Ensuring policies and procedures governing the collection and use of reported information are in accordance with all applicable laws and Executive Orders and include appropriate protections for privacy and civil liberties
- Analyzing, acting upon, and sharing reported information of a security, CI, or law enforcement concern with authorized security, insider threat, or law enforcement officials
- Sharing reported information that may result in an adverse determination of a covered individual's continued national security eligibility with security or CI officials of other agencies that have a direct interest in the covered individual
- Ensuring the providing of training and briefings on individual reporting obligations during employee indoctrination and in annual refresher training
- Cooperating with the SecEA in assessing the continued efficiency and effectiveness of current and any future reporting requirements

Supervisor

Supervisor responsibilities include:

- Monitoring the effectiveness of reporting requirements and developing recommendations for new and modified requirements
- Overseeing agency compliance
- Ensuring best practices are identified, shared, and implemented
- Continuously evaluating individuals with national security eligibility to determine if they continue to be trustworthy in accordance with SEAD 4
- Ensuring the accomplishment of security responsibilities is included in personnel performance evaluations, based on Section 552a of Title 5, United States Code and DOD Component guidance
- Reporting any derogatory information that falls within the adjudicative guidelines, such as government travel card misuse, misuse of IT systems, abuse, or fraud to their cognizant security professional or commander

Security Professionals

Security professionals are responsible for reporting unfavorable information to the appropriate adjudication facility, law enforcement, or CI supporting activity and forwarding the report to the adjudication facility via the system of record; reporting unfavorable information concerning cleared contractor personnel to the DCSA Consolidated Adjudication Services (CAS); Defense

Counterintelligence and Security Agency (DCSA); and to the contractor facility security officer (FSO); and providing details for all security incidents.

In the incident report, security professionals should include:

- The nature and seriousness of the conduct
- The circumstances surrounding the conduct
- The frequency and recency of the conduct
- The age of the individual at the time
- The extent participation was voluntary or willfulness of conduct
- The knowledge the individual had of the consequences
- The motivation for the conduct
- How the command became aware of the information
- Actions the individual has taken to correct the issue, including medical treatment, counseling, or lifestyle changes
- The stability of the individual's lifestyle or work performance, including demonstrative examples
- Cooperation on the part of the individual in following medical or legal advice or assisting in command efforts to resolve the security issue
- The command recommendation to the supporting adjudication facility on whether to retain an individual's eligibility based on the national security investigation or when rendering a final determination. Note that the individual must be provided a copy of that recommendation.

Employee

All employees are obligated to advise the appropriate authorities or officials when they become aware of any information, behavior, or conditions that may pose a security concern, or that raise doubts to whether a co-worker's eligibility or access to classified information or assignment to sensitive duties is consistent with national security. If it is proven that an employee failed to report facts about a co-worker, an adverse national security eligibility action may be initiated against the employee who failed to report it.

Individual

The ultimate responsibility for maintaining continued national security eligibility rests with individuals. Individuals should familiarize themselves with security regulations that pertain to their assigned duties. They should be aware of the standards of conduct required of persons with national security eligibility as well as the security requirements of their positions. They should recognize and

avoid the kind of personal behavior that would render them ineligible for continued access to classified information or assignment to sensitive positions. Personnel with access to classified information must protect classified information in their custody from unauthorized disclosure and be aware of and comply with CV and reporting requirements.

Review Activity 4

Hazel is a Senior Security Specialist at a DOD agency. A security incident occurred in which a subject mishandled protected information. Hazel is putting together a report on the incident. Which of the following details must Hazel provide in her incident report?

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

- ☐ Seriousness of the conduct
- ☐ Frequency and recency of the conduct
- ☐ Motivation of the conduct
- ☐ Witness testimony
- ☐ Corrective actions
- ☐ Recommendation whether to suspend subject

Review Activity 5

Frank is a supervisor at a DOD agency. While approving travel requests, he notices discrepancies with a subject's travel expenses including several unauthorized purchases. What action is Frank responsible for in this situation?

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

- ○ Providing a detailed security incident report to the DOD.
- ○ Removing the subject from access.
- ○ Reporting the information to his cognizant security professional.
- ○ No action is required as long as the subject reimburses the costs.

Review Activity 6

Allen is the head of a DOD agency. Which of the following security reporting tasks is Allen responsible for?

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

- ☐ Developing agency reporting guidance
- ☐ Providing training
- ☐ Developing new reporting requirements
- ☐ Maintaining reported information

Conclusion

Lesson Summary

You have completed the *Security Responsibilities and Duties* lesson. You should now be able to:

- Identify the security professional's responsibilities, including education and training requirements.
- Through situational examples, classify the duties and reporting requirements for all covered individuals who have access to classified information or hold a sensitive position.

Lesson 7: Practical Exercise

Introduction

Lesson Objectives

In this course, you learned about the key elements and considerations of the personnel security program (PSP), including position designation, investigative standards, adjudicative requirements, and the responsibilities and duties of security professionals. In this practical exercise you will have a chance to apply what you've learned.

Here are the lesson objectives.

- Through given scenarios, assess the requirements for successful and accurate position designation, including sensitivity levels of positions and any potential adverse effects on national security.
- Apply the Federal Personnel Vetting investigative standards and adjudications under TW 2.0 to a series of situational examples involving personnel.
- Apply the adjudication requirements for national security eligibility determinations through given scenarios involving military, contractors, and civilian personnel.
- Distinguish the security professional's responsibilities and duties in accordance with the PSP through given situations and scenarios.

Exercise Overview

A DOD security office is processing several subjects through the PSP. Can you help them through the major phases of the PSP? But first, take a moment to review position designation, investigations, adjudications, and the responsibilities and duties of security professionals.

Position Designation

Position designations correlate to the potentially adverse impact on national security. The Position Designation System (PDS) assesses the duties and responsibilities of a position to determine the degree of potential damage by misconduct of an incumbent of a position. Sensitivity levels include:

- Special-sensitive
- Critical-sensitive
- Non-critical sensitive
- Non-sensitive

The Position Designation Tool (PDT) is the tool used to guide personnel through the PDS process.

Investigations

Executive Order 10450 requires a background investigation to be conducted on each civilian officer or employee in any department or agency of the government.

The scope of the investigation will vary depending on the nature of the position, and degree of harm that could be caused by the individual in that position. The scope of investigation is directed by the three-tier investigative model:

- Low Tier (LT)
- Moderate Tier (MT)
- High Tier (HT)

In addition, the Federal Personnel Vetting Investigative Standards map the investigative requirements for five personnel vetting scenarios:

- Initial vetting
- Continuous vetting (CV)
- Upgrades
- Transfer of trust
- Re-establishment of trust

Adjudications

Adjudication is a process for making trust determinations.

National security adjudication is a personnel vetting process which seeks reasonable assurance that persons granted access to classified information, or hold sensitive positions, are loyal, trustworthy, and reliable.

When making trust determinations, adjudicators apply the Whole Person Concept, and utilize 13 National Security adjudicative guidelines and nine factors found in Security Executive Agent Directive 4 (SEAD 4).

Security Professionals

Security professionals have specific roles and responsibilities related to:

- Education and Training Programs
- Briefings
- Reporting Requirements

SEAD 3 outlines reporting requirements based on the following roles:

- Security Executive Agent (SecEA)
- Head of agency
- Supervisor
- Security professional
- Employee
- Individual

Position Designation Exercise

Position Designation

Let's meet our subjects.

Dalia Shah was recently promoted to Program Manager for the Army. As part of her duties, she requires eligibility for access to Secret Level information. In addition, her new role requires her to access automated systems of the Army active duty personnel, which contains PII.

Andrew Smith transferred from the National Security Agency (NSA) to the Defense Intelligence Agency (DIA). His position as Senior Intelligence Officer requires eligibility to Top Secret level classified information. In addition, his role requires he review counterintelligence (CI) investigations.

Sam Cruz was recently hired by the Defense Logistics Agency (DLA) as an Administrative Assistant. His role poses no potentially adverse effects on national security or effectiveness of service, and he does not require access to classified information.

Your first step is to determine the position designation category of each subject.

Subject: Dalia Shah

Role: Senior Program Manager for the Army

- Secret level eligibility
- Requires access to automated systems of the Army active duty personnel containing PII

Subject: Andrew Smith

Role: Senior Intelligence Officer for DIA

- Top Secret level eligibility
- Requires review of CI investigations

Subject: Sam Cruz

Role: Administrative Assistant for DLA

- No risk to national security or effectiveness of service
- No access to classified information

Activity 1

Using the information from each personnel profile, determine the appropriate designation category.

Question 1 of 3

Subject: Dalia Shah

Role: Senior Program Manager for the Army

- Secret level eligibility
- Requires access to automated systems of the Army active duty personnel containing PII

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

- ○ Special-sensitive
- ○ Critical-sensitive
- ○ Non-critical sensitive
- ○ Non-sensitive

Question 2 of 3

Subject: Andrew Smith

Role: Senior Intelligence Officer for DIA

- Top Secret level eligibility
- Require review of CI investigations

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

- ○ Special-sensitive
- ○ Critical-sensitive
- ○ Non-critical sensitive
- ○ Non-sensitive

Question 3 of 3

Subject: Sam Cruz

Role: Administrative Assistant for DLA

- No risk to national security or effectiveness of service
- No access to classified information

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

- ○ Special-sensitive
- ○ Critical-sensitive
- ○ Non-critical sensitive
- ○ Non-sensitive

Investigation Exercise

Investigation

Now that the position designation category is assigned for each subject, it is time to determine the scope of the background investigation for each subject. To do so, you must determine the appropriate investigative tier and personnel vetting scenario. Each subject's personnel folder has been updated with any new and relevant information.

Subject: Dalia Shah

Role: Senior Program Manager for the Army

- Secret level eligibility
- Requires access to automated systems of the Army active duty personnel containing PII
- **Non-critical sensitive level position**
- **Promoted to this position from within the agency from a non-sensitive position**
- **Has undergone an initial trust determination and been enrolled in compliant CV**

Subject: Andrew Smith

Role: Senior Intelligence Officer for DIA

- Top Secret level eligibility
- Requires review of CI investigations
- **Critical-sensitive level position**
- **Transferred from NSA to DIA**

Subject: Sam Cruz

Role: Administrative Assistant for DLA

- No risk to national security or effectiveness of service
- No access to classified information
- **Non-sensitive level position**
- **New hire (no previous government experience)**

Activity 2

Using the information from each personnel profile, determine the appropriate investigative tier.

Question 1 of 3

Subject: Dalia Shah

Role: Senior Program Manager for the Army

- Secret level eligibility
- Requires access to automated systems of the Army active duty personnel containing PII
- Non-critical sensitive level position
- Promoted to this position from within the agency from a non-sensitive position
- Has undergone an initial trust determination and been enrolled in compliant CV

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

- ○ Low Tier (LT)
- ○ Moderate Tier (MT)
- ○ High Tier (HT)

Question 2 of 3

Subject: Andrew Smith

Role: Senior Intelligence Officer for DIA

- Top Secret level eligibility
- Requires review of CI investigations
- Critical-sensitive level position
- Transferred from NSA to DIA

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

- ○ Low Tier (LT)
- ○ Moderate Tier (MT)
- ○ High Tier (HT)

Question 3 of 3

Subject: Sam Cruz

Role: Administrative Assistant for DLA

- No risk to national security or effectiveness of service
- No access to classified information
- Non-sensitive level position
- New hire (no previous government experience)

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

- ○ Low Tier (LT)
- ○ Moderate Tier (MT)
- ○ High Tier (HT)

Activity 3

Using the information from each personnel file, determine the appropriate vetting scenario.

Question 1 of 3

Subject: Dalia Shah

Role: Senior Program Manager for the Army

- Secret level eligibility
- Requires access to automated systems of the Army active duty personnel containing PII
- Non-critical sensitive level position
- Promoted to this position from within the agency from a non-sensitive position
- Has undergone an initial trust determination and been enrolled in compliant CV

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

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Question 2 of 3

Subject: Andrew Smith

Role: Senior Intelligence Officer for DIA

- Top Secret level eligibility
- Requires review of CI investigations
- Critical-sensitive level position
- Transferred from NSA to DIA

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

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Question 3 of 3

Subject: Sam Cruz

Role: Administrative Assistant for DLA

- No risk to national security or effectiveness of service
- No access to classified information
- Non-sensitive level position
- New hire (no previous government experience)

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

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Adjudication Exercise

Adjudication

The investigative service provider (ISP) completes the personnel security investigation on each subject and sends it to CAS for an eligibility determination. Each subject's file must now undergo a national security adjudication.

Review Activity 4

Which of the following information is likely related to a national security adjudicative guideline?

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

- ☐ Andrew discloses that he has undergone an alcohol treatment program and has been sober for the past five years.
- ☐ Dalia mentions her current volunteer work as a youth soccer coach for a U.S. soccer organization.
- ☐ Sam discusses a large amount of medical debt he incurred after a car accident three years ago. He is currently on a payment plan to resolve the debt.

Determination

All three subjects receive a favorable national security eligibility determination. However, the PSP process does not end there as the subjects will undergo continuous vetting. In addition, all covered individuals have reporting requirements.

Let's take a look at those next.

Security Professional Exercise

Security Professional

SEAD 3 establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position. Let's look at the reporting responsibilities for our subject Andrew. Andrew's personnel folder has been updated with any new and relevant information.

Subject: Andrew Smith

Role: Senior Intelligence Officer for DIA

- Top Secret level eligibility
- Requires he review CI investigations
- Critical-sensitive level position
- Transferred from NSA to DIA
- **National Security Determination: Favorable**
- **Top Secret level access**

Review Activity 5

Using the information from Andrew's personnel file determine his reporting requirements.

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

- ☐ Use of a foreign passport
- ☐ Adoption of U.S. citizen children
- ☐ Bankruptcy
- ☐ Blackmail
- ☐ Marriage

Conclusion

Lesson Summary

You have completed the *Practical Exercise* lesson. You should now be able to:

- Through given scenarios, assess the requirements for successful and accurate position designation, including sensitivity levels of positions and any potential adverse effects on national security.
- Apply the Federal Personnel Vetting investigative standards and adjudications under TW 2.0 to a series of situational examples involving personnel.
- Apply the adjudication requirements for national security eligibility determinations through given scenarios involving military, contractors, and civilian personnel.
- Distinguish the security professional's responsibilities and duties in accordance with the PSP through given situations and scenarios.

Lesson 8: Course Conclusion

Conclusion

Course Summary

The Personnel Security Program (PSP) aims to protect national security by ensuring that only loyal, trustworthy, and reliable individuals may access classified information or perform sensitive duties. During this course, we discussed the key elements and considerations of the PSP, including position designation, investigative standards, adjudications, and the responsibilities and duties of security professionals. This course has provided you tools and information to understand how personnel security helps protect our nation.

Lesson Review

Here is a list of the lessons in the course.

- Lesson 1: Course Introduction
- Lesson 2: Overview of Personnel Security
- Lesson 3: Position Designation
- Lesson 4: Investigations
- Lesson 5: Adjudications
- Lesson 6: Security Responsibilities and Duties
- Lesson 7: Practical Exercise

Lesson Summary

Congratulations! You have completed the *Introduction to Personnel Security* course. You should now be able to:

- Summarize the key elements of personnel security.
- Through given scenarios, assess the requirements for successful and accurate position designation, including the sensitivity levels of positions and any potential adverse effects on national security.
- Apply the Federal Personnel Vetting investigative standards and adjudications under TW 2.0 to a series of situational examples involving personnel.
- Apply the adjudication requirements for national security eligibility determinations through given scenarios involving military, contractors, and civilian personnel.

- Distinguish the security professional's responsibilities and duties in accordance with the PSP through given situations and scenarios.

To receive course credit you MUST take the *Introduction to Personnel Security* examination. Please use the STEPP system from the Center for Development of Security Excellence to access the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

Which of the following are key aspects of the Personnel Security Program (PSP)?

- ☐ Overseeing the competitive hiring system.
- ☑ Providing eligibility to access classified information. (correct response)
- ☑ Ensuring the protection of national security. (correct response)
- ☐ Managing the auditing of defense contractors.

***Feedback**: Two key aspects of the PSP are providing access to classified information and ensuring the protection of national security. The PSP aims to protect national security by ensuring that only loyal, trustworthy, and reliable individuals may access classified information and/or be assigned to national security sensitive positions.*

Review Activity 2

Which of the following are processes of personnel security?

- ○ Background investigations
- ○ Adjudications
- ○ Continuous vetting
- ⦿ All of the above (correct response)

***Feedback**: Personnel security consists of three distinct processes: background investigations, adjudications, and continuous vetting.*

Review Activity 3

Question 1 of 2. Which of the following Executive Orders (E.O.s) requires all persons who are employed by the government to be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States?

- ○ E.O. 10450, Security Requirements for Government Employment
- ⦿ E.O. 10865, Safeguarding Classified Information within Industry (correct response)
- ○ E.O. 13764, Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters
- ○ E.O. 13869, Transferring Responsibility for Background Investigations to the Department of Defense

***Feedback**: E.O. 10865 requires all persons who are employed by the government to be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States.*

Question 2 of 2. Which of the following Executive Orders (E.O.s) amends E.O. 13467 and E.O. 13488?

- ○ E.O. 10450, Security Requirements for Government Employment
- ○ E.O. 10865, Safeguarding Classified Information within Industry
- ⦿ E.O. 13764, Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters (correct response)
- ○ E.O. 13869, Transferring Responsibility for Background Investigations to the Department of Defense

***Feedback**: E.O. 13764 amends E.O. 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information" and E.O. 13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust".*

Review Activity 4

Which of the following policy documents guides the transformative efforts to reform the U.S government personnel security vetting process?

- ○ DOD Instruction (DODI) 5200.02, DOD Personnel Security Program
- ○ DOD Manual 5200.02 (DODM), Procedures for the DOD Personnel Security Program
- ⦿ Federal Personnel Vetting (FPV) Core Doctrine (correct response)
- ○ Security Executive Agency Directive (SEAD) 6: Continuous Evaluation (CE)

***Feedback**: The FPV Core Doctrine guides the transformative efforts to reform the U.S Government personnel security vetting process.*

Review Activity 5

Which of the following describes the purpose of TW 2.0?

- ☑ It provides a whole-of-government approach to reforming the personnel security process. (correct response)
- ☐ It provides a one phase process for onboarding federal contractors.
- ☑ It establishes a single vetting system for the U.S. government. (correct response)
- ☐ It revises the adjudication guidelines applied for national security purposes.

***Feedback**: TW 2.0 is the whole-of-government approach to reforming the personnel security process. It establishes a single vetting system for the U.S. government.*

Review Activity 6

Which of the following are key improvements under TW 2.0?

- ☑ Reducing time required to onboard new hires. (correct response)
- ☑ Simplifying workforce mobility. (correct response)
- ☑ Enhancing risk management. (correct response)
- ☐ Providing a universal approach to agency needs.

***Feedback**: Several improvements are made under TW 2.0 including reducing the time required to onboard new hires, simplifying workforce mobility, enhancing risk management by identifying potentially problematic behavior sooner than traditional vetting tools and processes, and improving the ability of personnel vetting programs to meet agency mission needs while considering unique agency-specific requirements.*

Review Activity 7

Which of the following best describes continuous vetting?

- ○ Periodic reinvestigations of an individual's background
- ○ Early investigations into an individual's background to determine eligibility for hire
- ○ Ongoing investigations only into individuals that pose a threat to national security
- ⦿ A near real-time review of an individual's background at any time (correct response)

***Feedback**: Continuous vetting is a near real-time review of an individual's background at any time to determine if they continue to meet their requirements to uphold eligibility to access classified information.*

Lesson 3 Review Activities

Review Activity 1

Lea is an Analyst who works at a DOD agency. She is a civilian who works on projects that have varying levels of impact on national security. One of her projects involves reviewing war plans that require access to Top Secret information. Which of the following categories describes Lea's civilian position?

- ○ Non-critical sensitive
- ⦿ Critical-sensitive (correct response)
- ○ Special-sensitive

***Feedback**: DOD civilian employee positions that require access to Top Secret information are designated critical-sensitive.*

Review Activity 2

Frank is a member of the Canadian Air Force. He is on a temporary assignment working at a DOD agency and needs access to classified information. Frank has unusual expertise and knowledge for a position that a U.S. citizen does not have. To be eligible to do the job, Frank receives which of the following?

- ○ Access
- ○ National Security eligibility
- ⦿ Limited Access Authorization (correct response)

***Feedback**: A non-U.S. citizen who requires access to classified information access to perform official duties can be granted a Limited Access Authorization.*

Lesson 4 Review Activities

Review Activity 1

Question 1 of 4

Subject: Isabel Armstrong

Role: Program Manager

- Non-critical sensitive position
- Requires access to Secret level classified information

- ○ Low Tier (LT)
- ⦿ Moderate Tier (MT) (correct response)
- ○ High Tier (HT)

***Feedback**: The MT includes positions designated as non-critical sensitive. For non-critical sensitive positions, the level of investigation can be used to grant access to classified information at the Secret level.*

Question 2 of 4

Subject: Alex Chang

Role: Human Resources Specialist

- Non-sensitive/Low risk
- Requires HSPD-12 Credentialing

- ⦿ Low Tier (LT) (correct response)
- ○ Moderate Tier (MT)
- ○ High Tier (HT)

***Feedback**: The LT positions designated as low-risk, non-sensitive, and is the minimum investigative tier for eligibility for physical and/or logical access or credentialing determinations. HSPD-12 Credentialing is included in this tier.*

Question 3 of 4

Subject: Christopher Ruiz

Role: Navy Engineer

- Special-sensitive position
- Requires access to Sensitive Compartmented Information (SCI)

- ○ Low Tier (LT)
- ○ Moderate Tier (MT)
- ⦿ High Tier (HT) (correct response)

***Feedback**: The HT includes positions designated as special-sensitive. For special-sensitive positions, the level of investigation can be used to grant access to SCI.*

Question 4 of 4

Subject: Zakiya Thomas

Role: Senior Intelligence Specialist

- Critical-sensitive position
- Requires access to Top Secret level classified information

- ○ Low Tier (LT)
- ○ Moderate Tier (MT)
- ⦿ High Tier (HT) (correct response)

***Feedback**: The HT includes positions designated as critical-sensitive. For critical-sensitive positions, the level of investigation can be used to grant access to classified information at the Top Secret level.*

Review Activity 2

Question 1 of 3. Dave is a program manager for a project for the Office of Naval Research. The project is coming to an end. To support mission needs, Dave is moved on to manage a project for the Naval Education and Training Command which is the same sensitivity level and requires the same level of access.

Which personnel vetting scenario is Dave subject to?

- ○ Initial Vetting
- ○ Continuous Vetting (CV)

- ○ Upgrades
- ⦿ Transfer of Trust (correct response)
- ○ Re-establishment of Trust

Feedback*: The Transfer of Trust vetting scenario is a process for ensuring that investigative information is available and accessible, as appropriate, when individuals transfer across departments or agencies and across roles.*

Question 2 of 3. Aria is an Intelligence Specialist for the National Security Agency (NSA). She has already undergone an initial trust determination and been enrolled in CV for her current position, which is a non-critical sensitive position with access to Secret level classified information. Aria accepts a new position as a Senior Intelligence Specialist within the NSA. This new position, however, is critical-sensitive and requires access to Top Secret level information.

Which personnel vetting scenario is Aria subject to?

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ⦿ Upgrades (correct response)
- ○ Transfer of Trust
- ○ Re-establishment of Trust

Feedback*: Upgrades occur when a subject has undergone an initial trust determination, been enrolled in compliant CV, and moves to a new position requiring a higher-level investigation within or on behalf of the same department or agency.*

Question 3 of 3. Van is a software engineer that left their DOD position to work for a private company. After one year in the private sector, Van returns to the DOD at the same position designation and sensitivity level

Which personnel vetting scenario is Dave subject to?

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ○ Upgrades
- ○ Transfer of Trust
- ⦿ Re-establishment of Trust (correct response)

Feedback*: Re-establishment of Trust is the process used for an individual who stops performing work for or on behalf of the federal government for a period of time.*

Lesson 5 Review Activities

Review Activity 1

Which of the following best describes what an adjudicator must do when making trust determinations?

- ○ Collect unfavorable information from a person's past.
- ○ Review a written narrative from the subject detailing their lived experience.
- ○ Review an individual's past employment history.
- ⦿ Examine all available and reliable information about the person, past and present, favorable and unfavorable. (correct response)

***Feedback**: When making national security eligibility trust determinations adjudicators must use the whole-person concept. This includes examining all available, reliable information about the person, past and present, favorable and unfavorable.*

Review Activity 2

Question 1 of 2. Review the scenario and determine the appropriate trust determination.

Logan was hired as a contractor for a DOD agency. What trust determination is used to determine whether Logan has the character or conduct necessary for the position?

- ○ Suitability adjudication
- ⦿ Fitness adjudication (correct response)
- ○ HSPD-12 adjudication

***Feedback**: Fitness adjudication determines whether an individual has the character and conduct necessary. Fitness adjudication is conducted for employees of contractors supporting the federal government.*

Question 2 of 2. Review the scenario and determine the appropriate trust determination.

Tanya was hired as an analyst for a DOD agency. She requires logical access to federal controlled information systems. What trust determination is used to issue credentials for logical access?

- ○ Suitability adjudication
- ○ Fitness adjudication
- ⦿ HSPD-12 adjudication (correct response)

***Feedback**: HSPD-12 adjudication determines who may be issued credentials for physical access to federal-controlled facilities or logical access to federal-controlled information systems.*

Review Activity 3

Review the scenario and determine the appropriate national security adjudicative guideline.

Lindsay is a newly assigned civilian employee who requires Top Secret eligibility. During a background investigation, an investigator interviewed Lindsay and learned that, when she was in college, she was the secretary of the New Free America Liberation Coalition. This group's goal is to overthrow the U.S. government and establish a worker state. This group seeks to achieve its goal through any means, including violence.

While Lindsay supported the concept of a worker state, she thought it would come about through the election process. When she learned the full extent of the group's goals, she left the organization.

What adjudicative guideline applies to this scenario?

- ⦿ A. Allegiance to the United States (correct response)
- ○ F. Financial considerations
- ○ I. Psychological Conditions
- ○ K. Handling Protected Information

***Feedback**: A. Allegiance to the United States applies to this scenario.*

Review Activity 4

Review the scenario and determine the appropriate national security adjudicative guideline.

John was born in the United States to British citizens who were legally residing and working in the United States at the time of his birth. He acquired British citizenship through his parents and has a current British passport. He is applying for a position in the U.S. government that requires Top Secret eligibility. As required, he disclosed his foreign citizenship and passport on his security form.

During the interview portion of his investigation, John disclosed that even though he was born in the United States, he holds British citizenship through his parents and maintains a British passport. He advised he only uses his U.S. passport when traveling to and from the United States. He also stated that he does not exercise any rights, privileges, or obligations associated with his foreign citizenship and does not hold any foreign financial or business interests.

What adjudicative guideline applies to this scenario?

- ⦿ C. Foreign Preference (correct response)
- ○ F. Financial considerations
- ○ I. Psychological Conditions
- ○ K. Handling Protected Information

***Feedback**: C. Foreign Preference applies to this scenario.*

Review Activity 5

Shannon is a civilian employee for a DOD agency. She is transferring to a position that is designated as higher risk and requires greater eligibility access than her current position, so she is being investigated for the upgrade. During the interview portion of her personnel security investigation, Shannon told the investigators that she purposefully omitted information about her involvement in a drug related crime.

According to due process for civilian employees, what must occur before an unfavorable national security eligibility determination is made?

- ☑ Shannon must be provided a Letter of Intent (LOI). (correct response)
- ☑ Shannon must be provided a Statement of Reasons (SOR). (correct response)
- ☐ The agency must audit the personnel security investigation.
- ☑ Shannon must be provided an opportunity to appeal. (correct response)
- ☐ The ISP must reinvestigate Shannon within 60 days.

Feedback*: An unfavorable national security eligibility determination will be rendered only after due process actions have been completed including providing the civilian employee with a LOI, a written SOR, and an opportunity to appeal the letter of denial (LOD).*

Review Activity 6

If the adjudication facility provides Shannon with a Letter of Denial (LOD) or Meritorious Waiver (LOR), what will be stated?

- ☑ Final determination of each adjudicative guideline that was provided in the Statement of Reasons (SOR) (correct response)
- ☑ What was mitigated or unmitigated (correct response)
- ☐ Steps to follow to appeal the decision
- ☑ Reason(s) for denying or revoking national security eligibility (correct response)

Feedback*: If Shannon receives an LOD or LOR, it must state the final determination of each adjudicative guideline that was provided to her in the SOR, what was mitigated or unmitigated, and the reason or reasons for denying or revoking her national security eligibility.*

Review Activity 7

At which point is an individual eligible for reconsideration following an unfavorable national security determination?

- ○ Immediately after the denial or revocation
- ○ 30 days following the denial or revocation
- ◉ 1 year following the denial or revocation (correct response)
- ○ 5 years following the denial or revocation

***Feedback**: For an unfavorable national security determination to be reconsidered, the individual's eligibility has to have been denied or revoked for at least 1 year.*

Review Activity 8

Which of the following is true regarding reinstating a DOD civilian after an unfavorable national security determination?

- ☑ Reinstatement must be in the interest of national security. (correct response)
- ☐ The security office makes the final determination on reinstatement.
- ☐ Reinstatement prevents the need for a new investigation.
- ☑ The DOD Component head can reinstate the employee. (correct response)
- ☐ The employee's supervisor may temporarily reinstate them.

***Feedback**: For an employee to be reinstated to a sensitive or national security position in the DOD, it must be in the interest of national security. Only the employee's DOD Component head can reinstate the employee.*

Lesson 6 Review Activities

Review Activity 1

Which of the following security professional briefings are completed annually and when there are changes to policies or procedures?

- ○ Initial Briefing
- ◉ Refresher Briefing (correct response)
- ○ Insider Threat Briefing
- ○ Termination Briefing

***Feedback**: A refresher briefing is done annually and when there are changes in security regulations, policies, or procedures.*

Review Activity 2

Question 1 of 2. Danielle is a civilian employee at the DOD in a non-critical sensitive position. According to SEAD 3 reporting requirements, what activities is Danielle responsible for reporting based on her position?

- ☐ U.S. citizen roommates
- ☑ Unofficial media contacts (correct response)
- ☑ Arrests (correct response)
- ☐ Adoption of non-U.S. citizen children
- ☑ Alcohol- and drug-related treatment (correct response)

***Feedback**: Individuals holding a non-critical sensitive position have additional reporting requirements including reporting unofficial media contacts, arrests, and alcohol- and drug-related treatment.*

Question 2 of 2. Sal is a military member of the DOD in a critical-sensitive position with access to Top Secret classified information. According to SEAD 3 reporting requirements, what activities is Sal responsible for reporting based on his position?

- ☐ U.S. citizen roommates
- ☑ Unofficial media contacts (correct response)
- ☑ Arrests (correct response)
- ☑ Adoption of non-U.S. citizen children (correct response)
- ☑ Alcohol- and drug-related treatment (correct response)

***Feedback**: Individuals with access to Top Secret information or holding a critical-sensitive position have additional reporting requirements including unofficial media contacts, arrests, adoption of non-U.S. citizen children, and alcohol- and drug-related treatment.*

Review Activity 3

Ronald is a contractor at a DOD agency. He is in a moderate-risk public trust position.

True or False. Ronald must receive approval from his agency head for any unofficial foreign travel.

- ○ True
- ⦿ False (correct response)

***Feedback**: An individual with Moderate-Risk Public Trust is not a covered individual according to SEAD 3.*

Review Activity 4

Hazel is a Senior Security Specialist at a DOD agency. A security incident occurred in which a subject mishandled protected information. Hazel is putting together a report on the incident. Which of the following details must Hazel provide in her incident report?

- ☑ Seriousness of the conduct (correct response)
- ☑ Frequency and recency of the conduct (correct response)
- ☑ Motivation of the conduct (correct response)
- ☐ Witness testimony
- ☑ Corrective actions (correct response)
- ☐ Recommendation whether to suspend subject

***Feedback**: Security professionals must provide several details when reporting a security incident including the seriousness of the conduct, frequency and recency of the conduct, motivation of the conduct, and actions the individual has taken to correct the issue.*

Review Activity 5

Frank is a supervisor at a DOD agency. While approving travel requests, he notices discrepancies with a subject's travel expenses including several unauthorized purchases. What action is Frank responsible for in this situation?

- ○ Providing a detailed security incident report to the DOD.
- ○ Removing the subject from access.
- ◉ Reporting the information to his cognizant security professional. (correct response)
- ○ No action is required as long as the subject reimburses the costs.

Feedback*: Supervisors are responsible for reporting any derogatory information that falls within the adjudicative guidelines including government travel card misuse to their cognizant security professional or commander.*

Review Activity 6

Allen is the head of a DOD agency. Which of the following security reporting tasks is Allen responsible for?

- ☑ Developing agency reporting guidance (correct response)
- ☑ Providing training (correct response)
- ☐ Developing new reporting requirements
- ☑ Maintaining reported information (correct response)

Feedback*: Heads of agencies have several responsibilities including developing agency reporting guidance, ensuring the providing of training regarding reporting obligations, and maintaining all reported information consistent with applicable law and policy.*

Lesson 7 Practical Exercise

Activity 1

Question 1 of 3

Subject: Dalia Shah

Role: Senior Program Manager for the Army

- Secret level eligibility
- Requires access to automated systems of the Army active duty personnel containing PII

- ○ Special-sensitive
- ○ Critical-sensitive
- ◉ Non-critical sensitive (correct response)
- ○ Non-sensitive

***Feedback**: Non-critical sensitive positions can cause significant damage to national security, including positions requiring eligibility for access to Secret level information and positions requiring access to automated systems that contain PII.*

Question 2 of 3

Subject: Andrew Smith

Role: Senior Intelligence Officer for DIA

- Top Secret level eligibility
- Require review of CI investigations

- ○ Special-sensitive
- ◉ Critical sensitive (correct response)
- ○ Non-critical sensitive
- ○ Non-sensitive

***Feedback**: Critical-sensitive positions are civilian national security positions that have the potential to cause exceptionally grave damage to the nation's security, including positions requiring eligibility for access to Top Secret level classified information and positions involving the handling of CI investigations.*

Question 3 of 3

Subject: Sam Cruz

Role: Administrative Assistant for DLA

- No risk to national security or effectiveness of service
- No access to classified information

- ○ Special-sensitive
- ○ Critical-sensitive
- ○ Non-critical sensitive
- ◉ Non-sensitive (correct response)

***Feedback**: Non-sensitive positions do not require access to classified information or performance of national security sensitive duties. These positions pose no potentially adverse effects on national security.*

Activity 2

Question 1 of 3

Subject: Dalia Shah

Role: Senior Program Manager for the Army

- Secret level eligibility
- Requires access to automated systems of the Army active duty personnel containing PII
- Non-critical sensitive level position
- Promoted to this position from within the agency from a non-sensitive position
- Has undergone an initial trust determination and been enrolled in compliant CV

○ Low Tier (LT)
⦿ Moderate Tier (MT) (correct response)
○ High Tier (HT)

Feedback*: The MT includes positions designated as non-critical sensitive. For non-critical sensitive positions, the level of investigation can be used to grant access to classified information at the Secret level.*

Question 2 of 3

Subject: Andrew Smith

Role: Senior Intelligence Officer for DIA

- Top Secret level eligibility
- Requires review of CI investigations
- Critical-sensitive level position
- Transferred from NSA to DIA

○ Low Tier (LT)
○ Moderate Tier (MT)
⦿ High Tier (HT) (correct response)

Feedback*: The HT includes positions designated as critical-sensitive. For critical-sensitive positions, the level of investigation can be used to grant access to classified information at the Top Secret level.*

Question 3 of 3

Subject: Sam Cruz

Role: Administrative Assistant for DLA

- No risk to national security or effectiveness of service
- No access to classified information
- Non-sensitive level position
- New hire (no previous government experience)

- ⦿ Low Tier (LT) (correct response)
- ○ Moderate Tier (MT)
- ○ High Tier (HT)

***Feedback**: The LT includes positions designated as low-risk, non-sensitive, and no risk to national security or effectiveness of service. LT is the minimum investigative tier for eligibility for physical and/or logical access.*

Activity 3

Question 1 of 3

Subject: Dalia Shah

Role: Senior Program Manager for the Army

- Secret level eligibility
- Requires access to automated systems of the Army active duty personnel containing PII
- Non-critical sensitive level position
- Promoted to this position from within the agency from a non-sensitive position
- Has undergone an initial trust determination and been enrolled in compliant CV

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ⦿ Upgrades (correct response)
- ○ Transfer of Trust
- ○ Re-establishment of Trust

***Feedback**: Upgrade trust vetting occurs when a subject has undergone an initial trust determination, been enrolled in compliant CV, and moves to a new position requiring a higher-level investigation within or on behalf of the same department or agency.*

Question 2 of 3

Subject: Andrew Smith

Role: Senior Intelligence Officer for DIA

- Top Secret level eligibility
- Requires review of CI investigations
- Critical-sensitive level position
- Transferred from NSA to DIA

- ○ Initial Vetting
- ○ Continuous Vetting (CV)
- ○ Upgrades
- ◉ Transfer of Trust (correct response)
- ○ Re-establishment of Trust

***Feedback**: The Transfer of Trust vetting scenario is a process for ensuring that investigative information is available and accessible, as appropriate, when individuals transfer across departments or agencies and across roles.*

Question 3 of 3

Subject: Sam Cruz

Role: Administrative Assistant for DLA

- No risk to national security or effectiveness of service
- No access to classified information
- Non-sensitive level position
- New hire (no previous government experience)

- ◉ Initial Vetting (correct response)
- ○ Continuous Vetting (CV)
- ○ Upgrades
- ○ Transfer of Trust
- ○ Re-establishment of Trust

***Feedback**: Initial vetting establishes trust with an agency.*

Review Activity 4

Which of the following information is likely related to a national security adjudicative guideline?

- ☑ Andrew discloses that he has undergone an alcohol treatment program and has been sober for the past five years. (correct response)
- ☐ Dalia mentions her current volunteer work as a youth soccer coach for a U.S. soccer organization
- ☑ Sam discusses a large amount of medical debt he incurred after a car accident three years ago. He is currently on a payment plan to resolve the debt. (correct response)

***Feedback**: Andrew and Sam's information would be evaluated based on national security adjudicative guidelines under G. Alcohol Consumption and F. Financial considerations.*

Review Activity 5

Using the information from Andrew's personnel file determine his reporting requirements.

- ☑ Use of a foreign passport (correct response)
- ☐ Adoption of U.S. citizen children
- ☑ Bankruptcy (correct response)
- ☑ Blackmail (correct response)
- ☑ Marriage (correct response)

***Feedback**: Individuals with access to Top Secret information or holding a critical-sensitive position have additional reporting requirements including reporting use of a foreign passport, blackmail, bankruptcy, and marriage.*