

***Introduction to Federal
Personnel Vetting Policy for
Security Practitioners***
Student Guide

October 2025

Center for Development of Security Excellence

Contents

| | |
|---|----|
| Introduction to Federal Personnel Vetting Policy for Security Practitioners | 1 |
| Lesson 1: Course Introduction | 3 |
| Course Introduction | 3 |
| Lesson 2: History of Personnel Vetting and Governing Authorities | 4 |
| Introduction | 4 |
| History Hall | 4 |
| Executive Actions | 7 |
| Lesson Conclusion..... | 13 |
| Lesson 3: Federal Personnel Vetting Policy Framework and Trusted Workforce 2.0..... | 15 |
| Introduction | 15 |
| Federal Personnel Vetting Policy and Trusted Workforce 2.0 Framework | 15 |
| Lesson Conclusion..... | 24 |
| Lesson 4: Personnel Vetting Domains and Federal Personnel Vetting Investigative Standards 25 | |
| Introduction | 25 |
| Personnel Vetting Domains | 25 |
| Investigative Tiers | 27 |
| Vetting Scenarios | 29 |
| Lesson Conclusion..... | 33 |
| Conclusion | 33 |
| Lesson 5: Course Conclusion | 34 |
| Conclusion | 34 |
| Appendix A: Answer Key..... | 36 |
| Lesson 2 Knowledge Checks..... | 36 |
| Lesson 3 Knowledge Checks..... | 37 |
| Lesson 4 Knowledge Checks..... | 39 |

Lesson 1: Course Introduction

Course Introduction

Welcome

Welcome to the Introduction to Federal Personnel Vetting Policy for Security Practitioners course and the Center for Development of Security Excellence (CDSE) Federal Personnel Vetting Library.

There are numerous policies and procedures that regulate and control the Federal Personnel Vetting program and ensure people, property, information, and mission (PPIM) are secure.

Your agency uses these policies to develop personnel vetting programs, manuals, and standard operating procedures (SOPs) that provide the procedures and processes to execute your job responsibilities.

Currently, there are personnel vetting (PV) reforms underway that are referred to as the Trusted Workforce (TW) 2.0 initiative. These reforms aim to better support agencies' missions by reducing the time required to onboard new hires, enabling mobility of the Federal workforce, and improving insight into workforce behaviors.

About This Course

As a security practitioner, you should be aware of the Federal Personnel Vetting-related policies and procedures that results in your agency's PV program manuals and SOPs. Also, because TW 2.0 will guide development of future Government-wide and agency policy, you need to be familiar with the TW 2.0 Federal Personnel Vetting policies and framework.

In this course, you will take a tour of the CDSE Federal Personnel Vetting library and learn about the different types of governing documents, spending most of your time in the Federal Personnel Vetting Policy room for an overview of the Federal Personnel Vetting Framework and TW 2.0 policies.

When you complete this course, you should be able to determine governing document types and principles related to the Federal Personnel Vetting program, as well as distinguish TW 2.0 policies within a hierarchy, and understand the Federal Personnel Vetting Policy Framework.

Here are the course objectives.

- Determine governing document types and principles related to the Federal Personnel Vetting program and incidents that have influenced the transformation of PV.
- Distinguish TW 2.0 policies within a hierarchy and understand the Federal Personnel Vetting Policy Framework.

Lesson 2: History of Personnel Vetting and Governing Authorities

Introduction

Lesson Objectives

Let's begin your tour of the CDSE Federal Personnel Vetting Library. You will start by visiting History Hall and then the Personnel Vetting Policy Stacks.

After you complete visiting those two sections of the library, you should be able to describe how laws and past events shape the Federal Personnel Vetting process and determine policies that govern the Federal Personnel Vetting program.

Here are the lesson objectives.

- Comprehend the past events that have impacted national security and prompted PV reform efforts.
- Determine policies that govern the Federal Personnel Vetting program, including U.S. laws, Executive Orders (E.O.s), Security Executive Agent Directives (SEADs), Intelligence Community Directives (ICDs), and Intelligence Community Policy Guidance (ICPG).

History Hall

Welcome to History Hall

Federal personnel vetting is the process by which individuals undergo investigation, evaluation, and adjudication by trusted Government personnel. Such personnel evaluate reliable and relevant information from background investigations and other reliable sources to make trust determinations or adjudicative decisions.

Federal personnel vetting encompasses the policies, processes, and tools used to determine whether individuals should be trusted to work for or on behalf of the Government, occupy a sensitive position or access classified information, and have access to Government information technology (IT) systems or facilities.

To understand the rationale behind the vetting process, you should be familiar with the history of these laws and congressional actions, which form the foundation of the Federal Personnel Vetting program.

Federal Laws and a Charter

Until now, the approach used for PV was developed over decades. However, PV reform modernizes transformational efforts in line with today's complex missions, societal norms, threat landscape, changing workforce, and evolving technology.

Now that we have defined Federal personnel vetting and its reform, review its history so you can understand the program's origins.

Here are three acts and a charter that form the Federal Personnel Vetting program's foundation.

Title VIII of the National Security Act of 1947

Establishes requirements for accessing classified information, including background checks and uniform standards.

Privacy Act of 1974

- Prohibits Federal agencies from disclosing information about an individual contained in a system of record without the prior written consent of that person.
- Requires agencies to maintain accurate and complete records and protect them from unauthorized use.
- Allows individuals to access their own personnel records.

Intelligence Reform and Terrorism Prevention Act of 2004

- Establishes a single department or agency (D/A) to be responsible for security clearances (referred to as security eligibility after the implementation of TW 2.0) and investigations.

- Requires all D/As to reciprocally accept background investigations and determinations and establishes an integrated, secure database on security clearances.

Trusted Workforce 2.0 Transforming Workforce Vetting Charter

- The Trusted Workforce (TW) 2.0 Transforming Workforce Vetting Charter, signed by Office of Personnel Management (OPM) and Office of the Director of National Intelligence (ODNI) was released in 2018, initiated the TW 2.0 initiative.
- TW 2.0 aims to better support agencies' missions by reducing the time required to bring new hires onboard, enabling mobility of the Federal workforce, and improving insight into workforce behaviors.

High-Profile Events

Many of the latest reforms to the Federal Personnel Vetting program, including the modern continuous vetting program, were spurred by attacks on national security from both insiders and adversaries overseas and threats from new and evolving technology.

Here are some past events that are the impetus to the transformational efforts of the Federal Personnel Vetting program, including the creation of the Defense Counterintelligence and Security Agency (DCSA), and TW 2.0.

These events highlight vulnerabilities in Federal personnel vetting and investigative processes, leading to reforms aimed at strengthening security, modernizing processes, and increasing efficiency.

Chelsea Manning, July 2013

Chelsea Manning, a former U.S. Army Intelligence Analyst, was convicted in July 2013 for leaking a massive trove of classified documents to WikiLeaks.

Aaron Alexis, September 2013

The Washington Navy Yard shooting on September 16, 2013, was a tragedy where Aaron Alexis, a former Navy Reservist and Information Technology contractor, fatally shot 12 people and injured 3 others. This incident raised significant concerns about the vetting process for individuals with national security eligibility and prompted calls for reforms in procedures to prevent similar tragedies in the future.

OPM Data Breach, 2014

In 2014, the OPM was the target of two data breaches, possibly conducted by state-sponsored attackers in China. Due to aging cybersecurity tools that prevented discovery of the attacks for many months, millions of employment and background investigation records were compromised.

NBIB Backlog, 2017

In 2017, the National Background Investigations Bureau (NBIB) had a background investigation backlog of over 700,000 cases. One of the contributing factors was the OPM data breach. The backlog caused significant delays in the adjudication and issuance of security eligibility.

Knowledge Check 1

Which document-initiated efforts to modernize and improve the efficiency of the personnel vetting process? *Select the best response. Check your answer in the Answer Key at the end of this Student Guide.*

- ☐ TW 2.0 Transforming Workforce Vetting Charter
- ☐ National Security Act of 1947
- ☐ Privacy Act of 1974
- ☐ Intelligence Reform and Terrorism Prevention Act of 2004

Knowledge Check 2

How did the Federal Personnel Vetting program change as a result of high-profile events like the OPM data breach, Washington Navy Yard Shooting, and NBIB investigative backlog? *Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.*

- ☐ The DCSA was established
- ☐ TW 2.0 was initiated
- ☐ Extra security practitioners were hired
- ☐ All applicants are provided interim eligibility

Executive Actions**Federal Laws**

Federal laws, also known as statutes or codes, are created by the legislative branch of the Government, such as Congress, and signed by the President. Laws define how people should

behave in areas that are under the authority of the Government to protect citizens' rights and ensure their safety.

Here are two Federal laws that you might see referenced in agency manuals, 50 United States Code (U.S.C.) Section 3341: Security Clearances and 5 U.S.C. Section 552, as amended: The Freedom of Information Act (FOIA).

50 U.S.C. § 3341 – Security Clearances

Establishes responsibility for direction of investigations and adjudications and reciprocity of trust determinations.

5 U.S.C. § 552 – The Freedom of Information Act (FOIA)

- FOIA allows individuals to request records from Federal agencies, including types of background checks and processes.
- Personnel files are generally exempted from FOIA requests to protect individual privacy.
- Exemptions for national security and law enforcement purposes may also apply.

Presidential Issuances

Presidential Issuances, such as Executive Orders (E.O.s) and Presidential Policy Directives (PPDs), are issued by the President of the United States and direct Federal Government operations.

Relevant E.O.s and an Executive Directive that apply to Federal personnel vetting are shown here.

E.O. 10450 (1953): Security Requirements for Government Employment

Requires that all persons employed in Government D/As be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States.

E.O. 10865, as amended (1960): Safeguarding Classified Information within Industry

Establishes appeal rights and procedures for industry applicants determined ineligible for access to classified information.

E.O. 12968, as amended (1995): Access to Classified Information and Background Investigative Standards

Establishes a uniform Federal personnel security program (PSP) for individuals considered for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.

Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors

- A standard badging process for Federal employees and contractors with the intention of enhancing security, reducing identity fraud, and protecting personal privacy.
- A process that, at a minimum, requires credentialing determinations of employees and contractors for access to Government-controlled facilities and information and the issuance of Personal Identification Verification (PIV) cards.

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

- Establishes personnel vetting policy and procedures for vetting individuals who work for or on behalf of the Federal Government.
- Aligns all vetting domains (suitability, fitness, national security, and credentialing).
- Authorizes continuous evaluation process for continued eligibility.
- Resulted in the creation of the Performance Accountability Council (PAC) to improve the Federal personnel vetting process, including the updating of outdated technology.
- Establishes Director of National Intelligence (DNI) as the Security Executive Agent (SecEA) and OPM as the Suitability Executive Agent (SuitEA).

E.O. 13488, as amended (2009): Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust

Establishes reinvestigation requirements for public trust positions and reciprocal acceptance of fitness determinations.

Presidential Policy Directive (PPD) 19 (2012): Whistleblower Protection

Ensures that employees serving in the Intelligence Community (IC) or who have national security eligibility and/or access can effectively report fraud, waste, and abuse without retaliation from their employer.

E.O. 13764 (2017): Amending the Civil Service Rules, E.O. 13488 and 13467 to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters

Provides the authorities needed to modernize, strengthen, and ensure a secure, efficient, and timely background investigation process that makes risk-based decisions and addresses evolving threats.

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

Department of Defense/Defense Counterintelligence and Security Agency (DOD/DCSA); establishes DCSA roles and responsibilities and other amendments to E.O. 13467.

Federal Regulations

Federal regulations, also known as rules, are created by the executive branch agencies to explain how to implement and interpret laws passed by Congress. Regulations are published first in the Federal Register and later included in the appropriate volume of the Code of Federal Regulation (CFR), which is the annual codification of all general and permanent rules.

Some CFRs that enforce and impact PV are shown here.

5 CFR Part 731 – Suitability and Fitness

Establishes regulations governing the Federal Government personnel vetting investigative and adjudicative processes for determining suitability and fitness. It also includes requirements and standards for agencies to properly vet individuals to assess risk to the integrity and efficiency of the service.

5 CFR Part 732 – National Security Positions

Establishes requirements and procedures for determining National Security, including position designation, investigation, and adjudication policy.

5 CFR Part 736 – Personnel Investigations

Establishes the requirements for personnel investigations conducted by the OPM, and for those conducted under delegated authority from OPM.

5 CFR Part 737 – Credentialing

Establishes the requirements for determining eligibility for PIV credentials commonly referred to as Common Access Card (CAC) in the DOD.

5 CFR Part 1400 – Designation of National Security Positions

Establishes position designations and investigation requirements.

32 CFR Part 117 – National Industrial Security Program Operating Manual (NISPOM)

Establishes requirements for cleared contractors under the National Industrial Security Program (NISP).

Security Executive Agent Directives

Security Executive Agent Directives (SEADs) are directives issued by the DNI as the SecEA. They contain uniform policies and procedures governing the conduct of investigations and national security adjudication for access to classified information and to occupy sensitive positions.

There are nine SEADs as shown here.

SEADs

- SEAD 1: Security Executive Agent Authorities and Responsibilities
- 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
- SEAD 3: Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position
- SEAD 4: National Security Adjudicative Guidelines

- SEAD 5: Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations
- SEAD 6: Continuous Evaluation
- SEAD 7: Reciprocity of Background Investigations and National Security Adjudications
- SEAD 8: Temporary Eligibility
- SEAD 9: Whistleblower Protection: Appellate Review of Retaliation Regarding Security Clearances and Access Determinations

Intelligence Community Directives and Policy Guidance

Intelligence Community Directives (ICDs) are established by the DNI. They provide policy and guidance to the intelligence community that governs operations and functions.

Intelligence Community Policy Guidance (ICPG) is a set of guidelines that dictate how the intelligence community conducts intelligence activities, handles sensitive information, and responds to specific situations, ensuring consistency across the entire intelligence apparatus.

ICDs and ICPGs that provide guidance for Federal personnel vetting are shown here.

ICDs and ICPGs

- ICD 704: Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information
- ICPG 704.1: Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information
- ICPG 704.3: Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes
- ICPG 704.4: Reciprocity of Personnel Security Clearance and Access Determinations

- ICPG 704.5: Intelligence Community Personnel Security Database Scattered Castles
- ICPG 704.6: Conduct of Polygraph Examinations for Personnel Security Vetting

Knowledge Check 3

Which E.O. resulted in the alignment of all vetting domains? Select the best response. *Check your answer in the Answer Key at the end of this Student Guide.*

- ☐ E.O. 12968, as amended (1995): Access to Classified Information and Background Investigative Standards
- ☐ E.O. 13467, as amended: Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information
- ☐ E.O. 13488, as amended: Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust
- ☐ E.O. 13764, Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, Credentialing, and Related Matters

Knowledge Check 4

Which uniform policy issued by DNI establishes the adjudicative criteria for individuals requiring eligibility to access classified information or eligibility to occupy a sensitive position? *Select the best response. Check your answer in the Answer Key at the end of this Student Guide.*

- ☐ 5 CFR 731: Suitability and Fitness
- ☐ E.O. 13869: Transferring Responsibility for Background Investigations to the Department of Defense
- ☐ SEAD 4: National Security Adjudicative Guidelines
- ☐ ICD 704.6: Conduct of Polygraph Examinations for Personnel Security Vetting

Lesson Conclusion

Lesson Summary

You have completed the History of Personnel Vetting and Governing Authorities lesson.

you should be able to:

- Comprehend the past events that have impacted national security and prompted PV reform efforts.
- Determine policies that govern the Federal Personnel Vetting program, including U.S. laws, E.O.s, SEADs, ICDs, ICPGs, and national policies.

Lesson 3: Federal Personnel Vetting Policy Framework and Trusted Workforce 2.0

Introduction

Lesson Objectives

In this section of the course, you will visit the Federal Personnel Vetting Policy Room of the library and review the purpose of Federal Personnel Vetting, its framework, and TW 2.0. You will also become familiar with the PV domains and attributes of a trusted insider and TW 2.0's strategic policies, guidelines, standards, and appendices.

Here is the lesson objective.

- Describe the purpose of Federal Personnel Vetting and TW 2.0 Framework.
- Define the PV domains and attributes of a trusted insider.
- Interpret TW 2.0 Strategic Policies.
- Interpret TW 2.0 Guidelines.
- Interpret TW 2.0 Implementing Standards at the Operational level.
- Interpret TW 2.0 Appendices at the Tactical level.

Federal Personnel Vetting Policy and Trusted Workforce 2.0 Framework

Purpose of the Federal Personnel Vetting and TW 2.0 Frameworks

The Security, Suitability, and Credentialing PAC is spearheading personnel vetting reforms under the TW 2.0 initiative. The DNI serving as the SecEA, and the Director of the OPM as the Suitability and Credentialing Executive Agent (Suit/Cred EA), provide joint EAs leadership. These reforms support agencies' missions by reducing the time required to bring new hires onboard, enabling mobility of the Federal workforce, and improving insight into workforce behaviors.

FPV and TW 2.0, the whole of Government reform, consists of one standard PV model, three investigative tiers, and five vetting scenarios. The One-Three-Five Framework applies across all personnel vetting domains.

One Personnel Vetting Model

Aligns the vetting processes with a simplified framework of Executive issuances, guidelines, and standards.

Three Investigative Tiers

Accelerate processing times, reduce duplication and complexity, and improve mobility.

Five Vetting Scenarios

Follow the lifecycle of an individual working for or on behalf of the Federal Government.

Federal Personnel Vetting Policy Framework

The Federal Personnel Vetting Policy Framework consists of a suite of policies organized in a top-down hierarchical structure with four levels, where each successive level is more agile.

At the top is the strategic level consisting of the TW 2.0 Federal Personnel Vetting Core Doctrine and TW 2.0 Executive Correspondences.

Next is the Guidelines level of policies. In alignment with the guiding principles of the Federal Personnel Vetting Core Doctrine, the Guidelines set of policies was issued by EAs in February 2022. They define the intended outcomes associated with investigations, adjudications, and personnel vetting management practices. They also describe the essential components for identifying and managing human risk to ensure a trusted workforce.

The Guidelines level includes the Federal Personnel Vetting, Federal Personnel Vetting Engagement, and Federal Personnel Vetting Performance Management Guidelines.

Beneath the Guidelines level are the Operational level policies. These policies are compliance-oriented and include such tools as the Federal Personnel Vetting Investigative, Common Principles in Applying Federal Personnel Vetting Adjudicative, Federal Personnel Vetting Management, and the Federal Personnel Vetting Performance Management Standards and Standard Forms.

The last level is Tactical in nature and includes appendices that are applied in the personnel vetting mission set of duties.

These policies include the Federal Personnel Vetting Investigative Standards Appendices, adjudicative criteria for all PV domains, Federal Personnel Vetting Management Standards Appendices, and the Federal Personnel Vetting Performance Management Standards Appendices.

Knowledge Check 1

What is 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.

- ☐ Reduce time to onboard new hires
- ☐ Enable workforce mobility between Federal agencies
- ☐ Add processes to the Federal Personnel Vetting program to prevent data breaches
- ☐ Improve identification of workforce behaviors that are inconsistent with those of a trusted person

Federal Personnel Vetting Policy

Federal Personnel Vetting Core Doctrine

At the Strategic level of the Federal Personnel Vetting Policy Framework is the Core Doctrine.

In February 2021, the EAs issued the Federal Personnel Vetting Core Doctrine, which guides the transformative efforts to reform the U.S. Government PV processes. It aligns, to the greatest extent practicable, the Federal workforce vetting processes to promote mobility, improve efficiencies, and move towards an enhanced risk management approach.

Trusted Workforce 2.0 Federal Personnel Vetting Core Doctrine

The Core Doctrine establishes the philosophy for the Government's personnel vetting program and will guide the development of Government-wide and agency policy. It defines the personnel vetting mission, its guiding principles, key supporting processes, and policy priorities.

TW 2.0 Executive Correspondences

The Executive Correspondences accompany the Core Doctrine and contains interim guidance and changes as the policies were developed.

Federal Personnel Vetting Guidelines

Now, let's take a closer look at the Guidelines and their subordinate documents, starting with the Federal Personnel Vetting Guidelines issued by the EAs in February 2021.

Federal Personnel Vetting Guidelines

This guideline describes the following:

- High-level outcomes for the Federal Personnel Vetting risk management framework
- How an individual is assessed against the characteristics of a trusted person
- Successful outcomes for the five PV scenarios
- Central elements of Federal Personnel Vetting

Federal Personnel Vetting Investigative Standards and Appendices

The Federal Personnel Vetting Process employs an investigative model that ensures that D/As have the necessary data and context to derive the needed information for making a determination of whether an individual is trusted to protect people, property, information, and mission.

The Federal Personnel Vetting Investigative Standards use investigative methodologies that seek attributes of a trusted individual and information types relevant to trust determinations as listed in the Federal Personnel Vetting Guidelines.

The Federal Personnel Vetting process includes an investigative model aligned to the attributes of a trusted individual who demonstrates:

- A regard for rules
- The ability to appropriately engage others
- Conduct consistent with the interests of the United States
- A willingness and ability to protect people, property, information, and mission

In May 2022, the EAs issued the requirements of this investigative model in the Federal Personnel Vetting Investigative Standards. These standards are in alignment with the Federal Personnel Vetting Guidelines and at the Operational level.

At the Tactical level, the Federal Personnel Vetting Investigative Standards has the nine appendices.

Federal Personnel Vetting Investigative Standards

- Create a risk management approach to investigations that maximizes uniformity across all four of the Federal Personnel Vetting domains and focuses on the efficient collection of information needed to make informed trust determinations.

- Focus information collection on obtaining the most relevant sources of information and put less emphasis on seeking specific numbers of each type of source.
- Include a description of the three investigative tiers and the five vetting scenarios.

Federal Personnel Vetting Investigative Standards Appendices

- Appendix A, Federal Personnel Vetting Information Types and Categories
- Appendix B, Initial Vetting Coverage Requirements
- Appendix C, Continuous Vetting Coverage Requirements
- Appendix D, Upgrades Coverage Requirements
- Appendix E, Transfer of Trust Coverage Requirements
- Appendix F, Re-establishment of Trust Coverage Requirements
- Appendix G, Issue and Case Seriousness Categorization
- Appendix H, Federal Personnel Vetting Investigative Methodologies
- Appendix I, Investigative Triggers and Required Actions

Common Principles in Applying Federal Personnel Vetting Adjudicative Standards

Also, at the Operational level with the Federal Personnel Vetting Investigative Standards are the Common Principles in Applying Federal Personnel Vetting Adjudicative Standards. These standards were issued by the EAs in July 2022.

Common Principles in Applying Federal Personnel Vetting Adjudicative Standards

- Describe the principles that are common across the four domains of suitability, fitness, national security, and credentialing.
- Introduce the whole person concept that stipulates that all available, reliable information about the person, past and present, favorable and unfavorable, should be considered in making trust determinations, where applicable.

SEAD 4 and 5 CFR Parts 731 and 737

Under the Common Principles for Applying Federal Personnel Vetting Adjudicative Standards falls SEAD 4: National Security Adjudicative Guidelines and 5 CFR Parts 731 and 737. These documents establish the adjudicative criteria security practitioners use to make preliminary trust determinations and adjudicators use to make final trust determinations.

SEAD 4: National Security Adjudicative Guidelines establish 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.

CFRs are general rules of the U.S. Federal Government, and they are organized into 50 titles. Title 5 governs administrative personnel that work in each Federal D/A, including OPM.

SEAD 4: National Security Adjudicative Guidelines

- Establish adjudicative criteria
- Pertain to all covered individuals
- Required for initial and continued eligibility

5 CFR Part 731: Suitability and Fitness

This part of 5 CFR establishes and maintains OPM's policies and procedures governing suitability and fitness investigations, adjudications, and continuous vetting requirements, including the procedures for taking and appealing suitability actions.

5 CFR Part 737: Credentialing

OPM proposed Part 737, and it determines the eligibility for PIV credentials under HSPD-12, to include adjudicative standards, requirements for suspension or revocation of eligibility for such credentials, and requirements for agencies to report all their PIV credentialing determinations to the Government-wide central repository.

Federal Personnel Vetting Management Standards and Appendices

The third standard that is at the Operational level under the Federal Personnel Vetting Guidelines is the Federal Personnel Vetting Management Standards.

The Federal Personnel Vetting Management Standards issued by EAs in July 2024 establish requirements for personnel vetting programs that ensure consistent approaches and practices to assess, determine, and manage the risk and trustworthiness of individuals who work for or on behalf of the Federal Government.

There are three appendices under the Federal Personnel Vetting Management Standards.

Federal Personnel Vetting Management Standards

All executive branch D/As execute the management standards across all domains (suitability, fitness, national security, and credentialing).

Consistent approaches and practices across the executive branch are essential to achieving the personnel vetting outcomes as specified in the Federal Personnel Vetting Guidelines.

Federal Personnel Vetting Management Standards Appendices

The Federal Personnel Vetting Management Standards have three appendices that describe PV activities that must be performed by Federal employees, required security awareness briefings, and types of information individuals must promptly report to D/As.

The appendices are:

- Appendix A: Personnel Vetting Business Functions
- Appendix B: Security Awareness
- Appendix C: Reporting Requirements for the Trusted Workforce

Federal Personnel Vetting Engagement Guidelines

There are two more Federal Personnel Vetting Guidelines that are part of the Policy Framework, Federal Personnel Vetting Engagement, and Federal Personnel Vetting Performance Management Guidelines.

Let's look at them and their supporting Operational and Tactical level documents now.

The Federal Personnel Vetting Engagement Guidelines contain direction for the Federal Personnel Vetting process that benefits from transparent, open, honest, and frequent communication necessary to establish and maintain a trusted workforce.

Standard Forms (SFs) are data collection questionnaires that individuals fill out as part of the PV process.

Federal Personnel Vetting Engagement Guidelines

The guidelines provide engagement components based on the five PV scenarios that you as a security practitioner implement to support individuals through the vetting process.

Standard Forms

Standard forms (SFs) include:

- SF-85: Questionnaire for Non-Sensitive Positions
- SF-85P: Questionnaire for Public Trust Positions
- SF-86: Questionnaire for National Security Positions

Under TW 2.0, the Personnel Vetting Questionnaire (PVQ) will replace these SFs implemented in the Electronic Application (eApp).

Federal Personnel Vetting Performance Management Guidelines, Standards, and Appendices

The Federal Personnel Vetting Performance Management Guidelines provide an overarching direction for a successful Federal Personnel Vetting program by collecting data to evaluate the effectiveness and efficiency of suitability, fitness, national security, and credentialing products, systems, and services to perform personnel vetting functions.

To determine the success and needs of PV programs, EAs and D/As collect various types of data as established in the Federal Personnel Vetting Performance Management Standards and Appendices.

Examples of collected data are the number of investigations in various stages and their outcomes, average times to complete investigations and resolve continuous vetting alerts, and number of determinations undergoing an appeal.

Federal Personnel Vetting Performance Management Standards

At the Operational level, the standards and its appendices establish the minimum measures used to quantify the success of PV programs across the enterprise.

Federal Personnel Vetting Performance Management Standards Appendices

The appendices are at the Tactical level and include:

- Appendix A: Performance Metrics
- Appendix B: Quality Management Programs

Federal Personnel Vetting Policy Framework Review

The Federal Personnel Vetting Core Doctrine provides the philosophy, goals, and priorities for all PV policy.

Derived from the Core Doctrine, the Federal Personnel Vetting, Federal Personnel Vetting Engagement, and Federal Personnel Vetting Performance Management Guidelines provide

high-level strategic direction and outcomes for the PV program. They show how the Core Doctrine is applied to produce the essential components of the program.

The standards at the Operational level establish the compliance requirements and principles. For example, the Federal Personnel Vetting Investigative Standards provide specific guidance and procedures for security practitioners and background investigators to collect sufficient information to meet the requirements of the PV program.

The Appendices and other documents at the Tactical level contain detailed information and requirements that implement the standards.

Knowledge Check 2

Match the Federal Personnel Vetting document type to its description. *Check your answer in the Answer Key at the end of this Student Guide.*

| Document Type | Description |
|------------------|--|
| A. Core Doctrine | 1. Tactical policies that are applied in the PV mission's set of duties and implement the standards |
| B. Guidelines | 2. Describe the outcomes of a successful vetting program |
| C. Standards | 3. Defines the personnel vetting mission, its guiding principles, key supporting processes, and policy priorities |
| D. Appendices | 4. Implement operational-level policies that include Federal Personnel Vetting investigative requirements, common principles, and standard forms |

Knowledge Check 3

What are the attributes of a trusted individual? *Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.*

- ☐ Demonstrates a regard for rules.
- ☐ Inappropriately engages others.
- ☐ Demonstrates willingness and ability to protect people, property, information, and mission.
- ☐ Demonstrates conduct consistent with the interest of the U.S.

Lesson Conclusion

Lesson Summary

You have completed the Federal Personnel Vetting Policy Framework and Trusted Workforce 2.0 lesson. You should now be able to:

- Describe the purpose of Federal Personnel Vetting and TW 2.0 Framework.
- Define the PV domains and attributes of a trusted insider.
- Interpret TW 2.0 Strategic Policies.
- Interpret TW 2.0 Guidelines.
- Interpret TW 2.0 Implementing Standards at the Operational level.
- Interpret TW 2.0 Appendices at the Tactical level.

Lesson 4: Personnel Vetting Domains and Federal Personnel Vetting Investigative Standards

Introduction

Lesson Objectives

We will remain in the Federal Personnel Vetting Policy Room of the CDSE Federal Personnel Vetting Library and explain the framework of the vetting program that is established in the policies. You will learn more about the PV domains, attributes of a trusted insider, the three-tier investigative framework, and the five vetting scenarios.

Here are the lesson objectives.

- Define the PV domains and attributes of a trusted insider.
- Explain the three-tier investigative framework of the Federal Personnel Vetting Investigative Standards.
- Explain the five vetting scenarios within the Federal Personnel Vetting Investigative Standards.

Personnel Vetting Domains

Four Personnel Vetting Domains

PV includes the process by which individuals undergo investigation, evaluation, and adjudication to determine if they possess the characteristics of a trusted person: good conduct, integrity, sound judgement, loyalty, and reliability.

PV is organized into four domains and considers position requirements and types of access. Although each domain has a distinct purpose and adjudicative criteria, the adjudication process culminates in a trust determination for any individual subject to personnel vetting.

Suitability

Suitability refers to a determination of whether the character or conduct of an individual may have an adverse impact on the integrity or efficiency of the service.

During the investigative process, the Investigative Service Provider (ISP) collects information relating to each of the criteria outlined in 5 CFR Part 731: Suitability and Fitness.

The potentially impacted positions when determining Suitability include competitive service, excepted service that cannot competitively convert to competitive service, or a career appointment to the Senior Executive Service.

The adjudicative process framework considers the whole-person concept utilizing the suitability and fitness factors along with additional considerations and culminates in a Suitability trust determination.

Fitness

Fitness refers to determinations of whether an individual's level of character and conduct are fit to work for, or on behalf of, a Federal agency.

During the investigative process, ISPs collect information relating to each of the criteria outlined in 5 CFR Part 731: Suitability and Fitness.

The positions for which Fitness is determined include excepted service positions, Non-Appropriated Fund (NAF) positions, and defense contractors.

The adjudicative process framework considers the whole-person concept utilizing the suitability and fitness factors along with additional considerations and culminates in a Fitness trust determination.

National Security

National security refers to a determination of whether an individual's eligibility for access to classified information or eligibility to hold a sensitive position is clearly consistent with the national security interest of the United States.

Any doubt about an individual's eligibility must be resolved in favor of national security.

During the investigative process, ISPs collect information relating to each of the criteria outlined in 5 CFR Part 732: National Security Positions.

The adjudicative process framework considers the whole-person concept utilizing SEAD 4: National Security Adjudicative Guidelines and additional factors; and culminates in a National Security trust determination.

Credentialing

Credentialing refers to a determination of whether an individual is eligible to obtain a HSPD-12 compliant PIV credential. In DOD, the credential is known as a CAC.

The primary purpose of credentialing 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 assets.

During the investigative process, ISPs collect information relating to each of the criteria outlined in HSPD-12 policy.

Credentialing confirms that the eligibility determination is consistent with protecting the life, safety, property, or health of individuals with access to Federal facilities and with protecting the Government's physical assets or information systems.

The adjudicative process framework considers the whole-person concept using the HSPD-12 Basic and Supplemental Standards and culminates in a credentialing trust determination.

Investigative Tiers

Three Investigative Tiers

The new Federal Personnel Vetting Investigative Standards establish a Three-Tier Investigative Model to replace the current five investigative tiers and streamline the investigative process.

The use of three tiers aligns investigative requirements for Federal Personnel Vetting for suitability, fitness, national security, and credentialing decisions and enable greater workforce mobility while simultaneously reducing duplication and complexity in the investigative process.

Each investigative tier builds upon the tier below it, with a mix of information categories and data sources that vary in complexity, coverage, and methodology commensurate with the increased risk at each investigative tier level.

Low Tier (LT)

LT is for Non-Sensitive/Low-Risk positions and is the equivalent to the current Tier 1 investigation.

LT is the minimum investigation tier for granting physical and/or logical access to facilities and making credentialing (HSPD-12) determinations.

Moderate Tier (MT)

MT is for Non-Sensitive/Moderate-Risk Public Trust and/or Non-Critical Sensitive/Moderate-Risk Public Trust positions and is the equivalent to the current Tier 2 and 3 investigations.

MT includes eligibility for access to Confidential and Secret information, or L-access.

High Tier (HT)

HT is for Non-Sensitive/High-Risk Public Trust and/or Critical-Sensitive/High-Risk Public Trust positions and is the equivalent to the current Tier 4 and 5 investigations.

HT includes eligibility for access to Top Secret information, Sensitive Compartmented Information (SCI), or Q-access.

| Previous Tier | Position Designations by Tier |
|---------------|--|
| Tier 1 | Low Risk Non-Sensitive Physical and Logical Access (HSPD-12) Credentialing |
| 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 (SCI) Q-access |

| TW 2.0 Tier | Position Designations by Tier |
|---------------|---|
| Low Tier | Non-Sensitive/Low Risk Physical and Logical Access (HSPD-12) Credentialing |
| Moderate Tier | Non-Sensitive/Moderate-Risk Public Trust Non-Critical Sensitive/Moderate-Risk Public Trust No National Security sensitivity |

| | |
|-----------|--|
| | Non-Sensitive/Moderate-Risk Critical-Sensitive/High-Risk Public Trust Secret/Confidential L-access |
| High Tier | Non-Sensitive/High-Risk Public Trust No National Security sensitivity |
| | Critical-Sensitive/High-Risk Public Trust Special-Sensitive/High-Risk Public Trust Top Secret Sensitive Compartmented Information Q-access |

Vetting Scenarios

Five Vetting Scenarios

The 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 personal history information.

All Federal Personnel Vetting falls within one of five personnel vetting scenarios in which information about individuals is collected and evaluated to make a trust determination. The five personnel vetting scenarios, as defined by the Federal Personnel Vetting Guidelines, are initial vetting, continuous vetting, upgrades, transfer of trust, and re-establishment of trust.

Initial Vetting

Initial vetting occurs when an individual is first assigned to a position of trust, usually upon beginning employment. It is commonly referred to as establishing trust.

Initial vetting is based upon the investigative tier for the position designation in accordance with Title 5 CFR, Parts 731, Suitability and Fitness and 1400, Designation of National Security Positions. You must ensure each position receives a risk and sensitivity designation according to the Position Designation System (PDS).

Tasks you complete in this scenario:

- Conduct vetting that establishes trust with an individual not previously vetted.
- Assess whether an individual can be trusted to protect PPIM.

- D/As may make a preliminary determination to onboard individuals based on the early results of high-yield record checks.

Information gathered during initial vetting provides insight and is used as a baseline for continuous vetting (CV).

Continuous Vetting

CV occurs on an ongoing basis with automated data source checks and investigative activities at intervals based on the investigative tier for the position designation.

- Assesses risk in near real time.
- Provides insight into trusted insider behavior.
- Maintains Federal Government's confidence that an individual will continue to protect PPIM.
- Allows D/As to implement remediation activities to assist the trusted insider before concerns escalate.
- Individuals consent to CV by certifying the PVQ or SF and are enrolled in CV after a favorable trust determination is made and recorded.

Upgrades

Upgrades occur when an individual requires a higher level of trust within the same agency when changing positions or assuming responsibilities at a higher tier than their existing trust determination.

The level of additional vetting needed is based on that which is required to meet the new investigative tier.

Transfer of Trust

Transfer of Trust (ToT) is a process applied when individuals move from one agency to another, commonly referred to as reciprocity.

Agencies must accept a favorable determination from another agency if it is for the same type of trust determination, such as national security, suitability, fitness, or credentialing, and it is at the appropriate level for the new position.

Types of transfers:

- A Federal employee or contractor moves to a new D/A

- A Federal employee or contractor moves to a new component within the same D/A
- A Federal employee becomes a contractor, or a contractor becomes a Federal employee
- A contractor moves from one contract company to another (even if sponsored by the same D/A)
- The sponsoring D/A of a contractor's company changes
- A contractor's D/A sponsor changes

Re-Establishment of Trust

The Re-establishment of Trust (RoT) process applies when former trusted insiders stop performing work for or on behalf of the Federal Government for a period of time and then seek to return.

Once fully implemented under TW 2.0, the break in service increases from 24 months to 36 months.

Goals of this scenario:

- Requires only the necessary level of PV
- Eliminates redundant PV actions
- Removes impediments to the re-entry and onboarding of former trusted insiders
- Tailors the degree of PV to address:
 - New position designation
 - Length of time the individual has not been affiliated with the Federal Government, commonly referred to as break in service
 - Individual's prior PV record

Knowledge Check 1

Match the personnel vetting domain with the correct description. *Check your answers in the Answer Key at the end of this Student Guide.*

| PV Domains | Description |
|----------------|---|
| A. Suitability | 1. Applies when an individual requires physical access to Federal facilities or logical access to Government systems. |

| PV Domains | Description |
|----------------------|--|
| B. Fitness | 2. Ensure that Government contractors or NAF employees demonstrate necessary character and conduct to work for, or on behalf of, a Federal agency. |
| C. National Security | 3. Ensures the character and conduct of the individual will promote the integrity and efficiency of the service. |
| D. Credentialing | 4. Applies when an individual requires eligibility to hold a sensitive position or eligibility to access classified information. |

Knowledge Check 2

Skyler is being vetted for a Non-Critical Sensitive/Moderate-Risk position that requires eligibility to access classified information at the Secret level. Which investigative tier is applied to this scenario? *Check your answer in the Answer Key at the end of this Student Guide.*

- ☐ Low Tier
- ☐ Moderate Tier
- ☐ Moderate/High Tier
- ☐ High Tier

Knowledge Check 3

Match the vetting scenario with the correct description. *Check your answers in the Answer Key at the end of this Student Guide.*

| PV Scenario | Description |
|-----------------------|---|
| A. Initial Vetting | 1. Vetting of individuals in near real-time to ensure they can be trusted to protect PPIM. |
| B. Continuous Vetting | 2. Also referred to as reciprocity, when individuals' trust determination follows them to another agency. |
| C. Upgrades | 3. Vetting of individuals who require a higher level of trust within the same agency. |

| PV Scenario | Description |
|------------------------------|---|
| D. Transfer of Trust | 4. Vetting of former trusted individuals who left but are returning to a Federal position. |
| E. Re-establishment of Trust | 5. Vetting of individuals for the first time to assess whether they can be trusted to protect PPIM. |

Lesson Conclusion

Conclusion

Lesson Summary

You have completed the Personnel Vetting Domains and Federal Personnel Vetting Investigative Standards lesson. You should now be able to:

- Define the PV domains and attributes of a trusted insider.
- Explain the three-tier investigative framework of the Federal Personnel Vetting Investigative Standards.
- Explain the five vetting scenarios within the Federal Personnel Vetting Investigative Standards.

Lesson 5: Course Conclusion

Conclusion

Course Summary

Congratulations! You have completed the Introduction to Federal Personnel Vetting Policy for Security Practitioners course. We hope you enjoyed your visit to the CDSE Federal Personnel Vetting Library. Let's take a moment to review what you learned.

You started your tour at History Hall where you visited the Federal Laws and High-Profile Events exhibits that illustrated how laws and past events laid the foundation for the Federal Personnel Vetting program.

Then, you visited the Personnel Vetting Policy Stacks and reviewed laws, regulations, and policies that govern the Federal Personnel Vetting program.

You completed your tour of the library in the Federal Personnel Vetting Policy Room where you described the Federal Personnel Vetting Policy Framework, defined personnel vetting domains, and interpreted TW 2.0 policies at the strategic, guidelines, operational, and tactical levels. You also learned about the Federal Personnel Vetting Investigative Standards, its three-tier investigative framework, and five vetting scenarios.

Lesson Review

Here is a list of the lessons in the course.

- Lesson 1: Course Introduction
- Lesson 2: History of Personnel Vetting and Governing Authorities
- Lesson 3: Federal Personnel Vetting Policy Framework and Trusted Workforce 2.0
- Lesson 4: Personnel Vetting Domains and Federal Personnel Vetting Investigative Standards

Course Summary

Now that you completed *Introduction to Federal Personnel Vetting Policy for Security Practitioners*, you should be able to:

- Determine governing document types and principles related to the Federal Personnel Vetting program and incidents that have influenced the transformation of PV.
- Distinguish TW 2.0 policies within a hierarchy and understand the Federal Personnel Vetting Policy Framework.

To receive course credit, you MUST take the *Introduction to Federal Personnel Vetting Policy for Security Practitioners* examination. Please use the Security, Training, Education, and Professionalization Portal (STEPP) system from the CDSE.edu to access the online exam.

Appendix A: Answer Key

Lesson 2 Knowledge Checks

Knowledge Check 1

Which document-initiated efforts to modernize and improve the efficiency of the personnel vetting process?

- ☒ TW 2.0 Transforming Workforce Vetting Charter (correct response)
- ☐ Intelligence Reform and Terrorism Prevention Act of 2004
- ☐ National Security Act of 1947
- ☐ Privacy Act of 1974

Feedback: In 2018, the DNI and Director of OPM launched TW 2.0 with the goal of promoting mobility, improving efficiencies, and developing an enhanced risk management approach.

Knowledge Check 2

How did the Federal Personnel Vetting program change as a result of high-profile events like the OPM data breach, Washington Navy Yard Shooting, and NBIB investigative backlog?

- ☒ The DCSA was established (correct response)
- ☒ TW 2.0 was initiated (correct response)
- ☐ Extra security practitioners were hired
- ☐ All applicants are provided interim eligibility

Feedback: After a series of high-profile events, the DCSA was established to oversee personnel vetting and TW 2.0 was initiated to improve the effectiveness and efficiency of the Federal Personnel Vetting program.

Knowledge Check 3

Which E.O. resulted in the alignment of all vetting domains?

- ☐ E.O. 12968, as amended (1995): Access to Classified Information and Background Investigative Standards
- ☒ E.O. 13467, as amended: Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (correct response)

- ☐ E.O. 13488, as amended: Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust
- ☐ 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

Feedback: E.O. 13467 requires the alignment of all vetting domains, authorized continuous evaluation, and established DNI as the Security Executive Agent and OPM as the Suitability Executive Agent.

Knowledge Check 4

Which uniform policy issued by DNI establishes the adjudicative criteria for individuals requiring eligibility to access classified information or eligibility to occupy a sensitive position?

- ☐ 5 CFR 731: Suitability and Fitness
- ☐ E.O.13869: Transferring Responsibility for Background Investigations to the Department of Defense
- ☒ SEAD 4: National Security Adjudicative Guidelines (correct response)
- ☐ ICD 704.6: Conduct of Polygraph Examinations for Personnel Security Vetting

Feedback: SEAD 4, issued by the DNI, establishes the national security adjudicative guidelines for individuals requiring eligibility to access classified information or eligibility to occupy a sensitive position.

Lesson 3 Knowledge Checks

Knowledge Check 1

What is the purpose of TW 2.0?

- ☒ Reduce time to onboard new hires (correct response)
- ☒ Enable workforce mobility between Federal agencies (correct response)
- ☐ Add processes to the Federal Personnel Vetting program to prevent data breaches
- ☒ Improve identification of workforce behaviors that are inconsistent with those of a trusted person (correct response)

Feedback: TW 2.0 aligns the Federal Personnel Vetting program's vetting processes with a simplified framework of Executive issuances, guidelines, and standards to improve the effectiveness and efficiency of the program.

Knowledge Check 2

Match the Federal Personnel Vetting document type to its description.

| Document | Correct Response |
|------------------|--|
| A. Core Doctrine | 3. Defines the personnel vetting mission, its guiding principles, key supporting processes, and policy priorities |
| B. Guidelines | 2. Describe the outcomes of a successful vetting program |
| C. Standards | 4. Implement operational-level policies that include Federal Personnel Vetting investigative requirements, common principles, and standard forms |
| D. Appendices | 1. Tactical policies that are applied in the PV mission's set of duties and implement the standards |

Feedback: The Federal Personnel Vetting Policy Framework is organized in a top-down hierarchical structure with the Core Doctrine at the strategic level (A3), Guidelines at the Guidelines level (B2), Standards at the Operational level (C4), and Appendices at the Tactical level (D1).

Knowledge Check 3

What are the attributes of a trusted individual?

- ☒ Demonstrates a regard for rules. (correct response)
- ☒ Inappropriately engages others. (correct response)
- ☐ Demonstrates willingness and ability to protect people, property, information, and mission.
- ☒ Demonstrates conduct consistent with the interest of the U.S. (correct response)

Feedback: The attributes of a trusted individual are listed in the Federal Personnel Vetting Investigative Standards and states the attributes of a trusted individual demonstrates regard for rules, appropriately engages others, demonstrates conduct consistent with the interest of the U.S., and demonstrates willingness and ability to protect people, property, information, and mission.

Lesson 4 Knowledge Checks

Knowledge Check 1

Match the personnel vetting domain with the correct description.

| PV Domain | Correct Response |
|----------------------|---|
| F. Suitability | 3. Ensures the character and conduct of the individual will promote the integrity and efficiency of the service. |
| G. Fitness | 2. Ensures that Government contractors or NAF employees demonstrate necessary character and conduct to work for, or on behalf of, a Federal agency. |
| H. National Security | 4. Applies when an individual requires eligibility to hold a sensitive position or eligibility to access classified information. |
| I. Credentialing | 1. Applies when an individual requires physical access to Federal facilities or logical access to Government systems. |

Feedback: Suitability determines if an individual can carry out the duties of a Federal job with integrity and efficiency (A3); fitness applies to Government contractors or NAF employees (B2); national security applies when an individual requires eligibility to hold a sensitive position or access to classified information (C4); and credentialing applies when an individual requires physical or logical access (D1).

Knowledge Check 2

Skyler is being vetted for a Non-Critical Sensitive/Moderate-Risk position that requires eligibility to access classified information at the Secret level. Which investigative tier is applied to this scenario?

- ☐ Low Tier
- ☒ Moderate Tier (correct response)
- ☐ Moderate/High Tier

○ High Tier

Feedback: Jobs that require access to Secret information are considered Non-Critical-Sensitive/Moderate-Risk Public Trust positions and utilize a moderate tier investigation.

Knowledge Check 3

Match the vetting scenario with the correct description.

| PV Scenario | Correct Response |
|------------------------------|---|
| A. Initial Vetting | 5. Vetting of individuals for the first time to assess whether they can be trusted to protect PPIM. |
| B. Continuous Vetting | 1. Vetting of individuals in near real time to ensure they can be trusted to protect PPIM. |
| C. Upgrades | 3. Vetting of individuals who require a higher level of trust within the same agency. |
| D. Transfer of Trust | 2. Also referred to as reciprocity, when individuals' trust determination follows them to another agency. |
| E. Re-establishment of Trust | 4. Vetting of former trusted individuals who left but are returning to a Federal position |

Feedback: Initial vetting is vetting an individual for the first time (A5); continuous vetting occurs in near real time (B1); upgrades are for individuals who need a higher level of trust (C3); transfer of trust is also known as reciprocity (D2); and re-establishment of trust occurs when individuals return after a break in service (E4).