February
2026

INTRODUCTION TO FEDERAL PERSONNEL VETTING POLICY FOR SECURITY PRACTITIONERS

QUICK REFERENCE GUIDE

TABLE OF CONTENTS

LESSON 1: INTRODUCTION

WELCOME

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.

Currently, there are personnel vetting (PV) reforms underway that are referred to as the Trusted Workforce 2.0 (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.

As a security practitioner, you should be aware of the Federal Personnel Vetting-related policies and procedures that drive and govern your agency's personnel vetting programs. TW 2.0 will guide the development of future Government-wide and agency policy; you need to be familiar with the TW 2.0 Federal personnel vetting policies and program frameworks.

LESSON 2: HISTORY OF PERSONNEL VETTING AND GOVERNING AUTHORITIES

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.

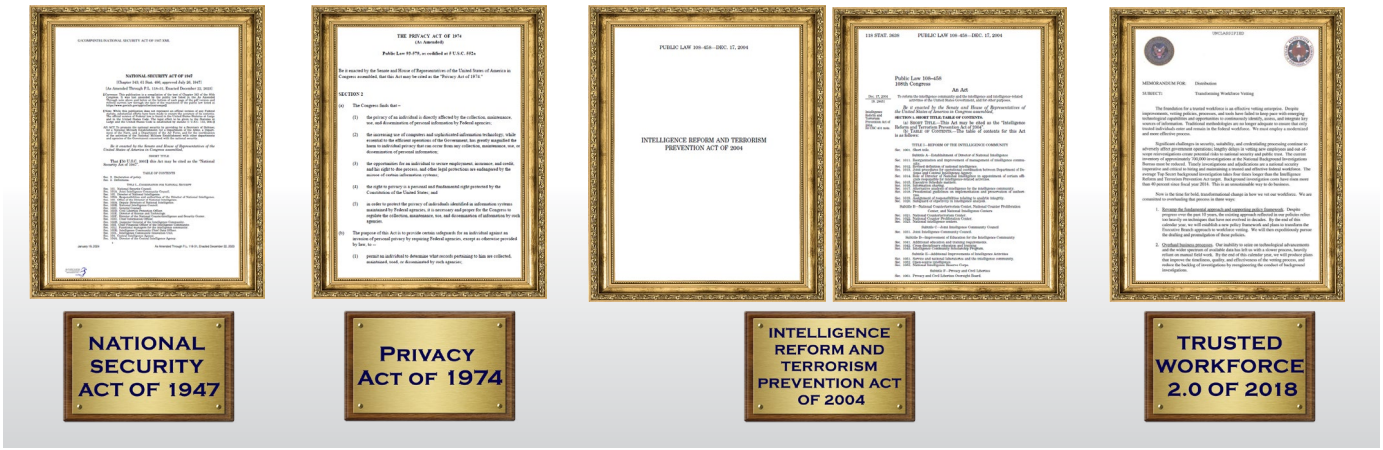
WHAT IS FEDERAL PERSONNEL VETTING?

Federal Personnel Vetting is the process by which trusted government personnel evaluate reliable and relevant information from background investigations and other reliable sources to make trust determinations or adjudicative decisions.

HISTORY OF PERSONNEL VETTING

FEDERAL LAWS AND A CHARTER

The approach used for PV developed over decades starting with these laws:



- **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.

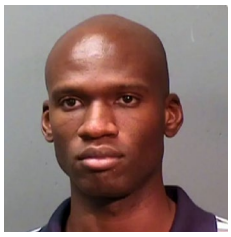
- **Trusted Workforce 2.0 Transforming Workforces Vetting Charter**
  - The Trusted Workforce 2.0 Transforming Workforce Vetting Charter, released in 2018, initiated the TW 2.0 initiative.
  - TW 2.0 aims to better support agencies' missions by reducing the time required to bring new hires onboard, enabling 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.

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 three 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 Office of Personnel Management (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.

GOVERNING AUTHORITIES

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.

Table 1: Personnel Vetting-Related Federal Laws

Law Title	Description
50 U.S.C. § 3341 – Security Clearances	Establishes responsibility for direction of investigations and adjudications, and reciprocity of trust determinations.
50 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.

Table 2: Personnel Vetting-Related Presidential Issuances

Presidential Issuance Title	Description
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 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 evalution process for continued eligibility. • Resulted in the creation of a performance accountability council (PAC) to improve the federal personnel vetting process including the updating of outdated technology. • Establishes the Director of Natioanl Intelligence (DNI) as the Security Executive Agent and OPM as the Suitability Executive Agent.

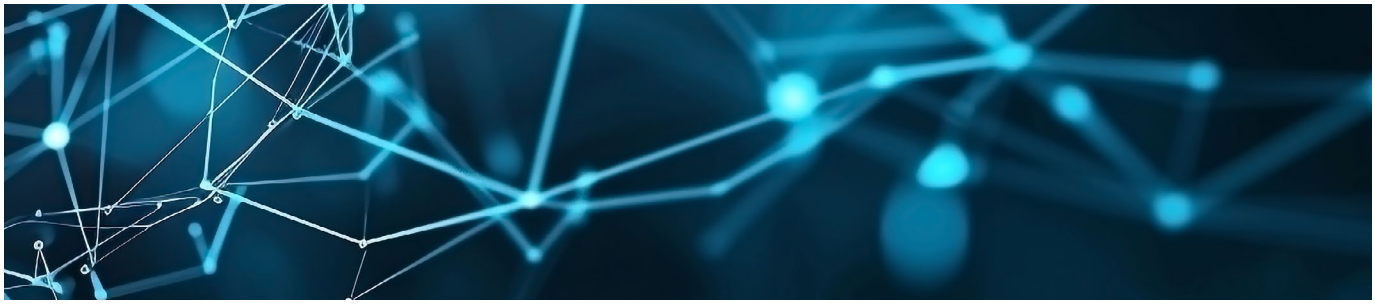
Presidential Issuance Title	Description
E.O. 13488, as amended (2009): Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust	Establishes reinvestigation requirements for public trust positions and reciprocal acceptance 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	Transfers NBIB investigative functions, personnel and resources to the Department of Defense/ Defense Counterintelligence and Security Agency (DoD/DCSA); establishes DCSA roles and responsibilities, and other amendments to EO 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.

Table 3: Personnel Vetting-Relate Federal Regulations

Presidential Issuance Title	Description
5 Code of Federal Regulation (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 Department of Defense (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 Security Executive Agent (SecEA). They contain uniform policies and procedures governing the conduct of investigations and national security adjudication for access to classified information and/or to occupy sensitive positions.

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 PROGRAM 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 Program Guidance (ICPGs) are 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.

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

LESSON 3: FEDERAL PERSONNEL VETTING POLICY FRAMEWORK AND TRUSTED WORKFORCE 2.0

PURPOSE OF FEDERAL PERSONNEL VETTING REFORMS

Federal Personnel Vetting policies and TW 2.0 aim 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.

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 OPM, serving as the Suitability and Credentialing Executive Agent (Suit/Cred EA) provide joint Executive Agents (EAs) leadership.

Security Executive Agent (SecEA)

+

Suitability and Credentialing Executive Agent (Suit/Cred EA)

→ **Executive Agents (EAs)**

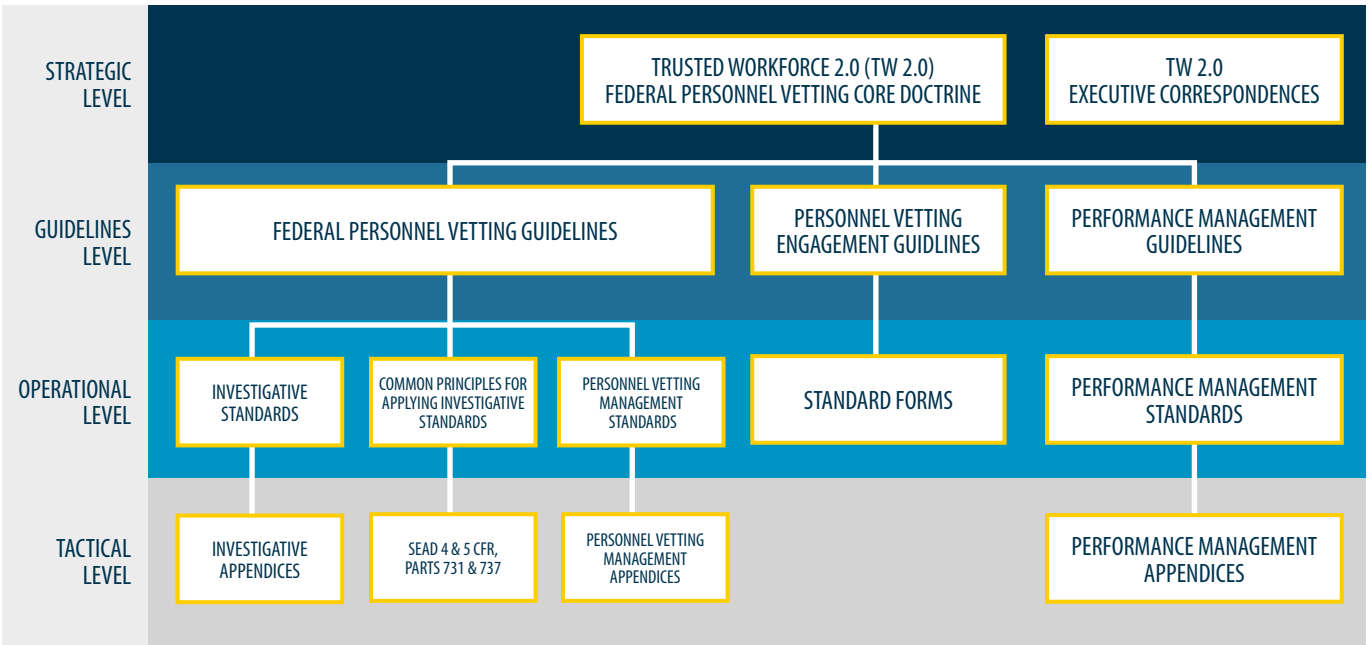
ONE-THREE-FIVE FRAMEWORK

Federal Personnel Vetting and TW 2.0 reform consists of one standard set of PV policy across the federal government, three investigative tiers, and five vetting scenarios. The One-Three-Five Framework applies across all vetting domains.

1 PERSONNEL VETTING MODEL	One Personnel Vetting Model aligns the vetting processes with a simplified framework of Executive issuances, guidelines, and standards.
3 INVESTIGATIVE TIERS	Three Investigative Tiers accelerate processing times, reduce duplication and complexity, and improve mobility.
5 VETTING SCENARIOS	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 Personnel Vetting Model consists of a suite of policies organized in a top-down hierarchical structure with four levels, where each successive level is more agile.



FEDERAL PERSONNEL VETTING CORE DOCTRINE

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

Trusted Workforce 2.0 Federal Personnel Vetting Core Doctrine

Establishes the philosophy for the Government's personnel vetting program and guides 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

Next is the Guidelines level of policies. In alignment with the guiding principles of the FPV 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.

Federal Personnel Vetting Guidelines

- 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

Under the Federal Personnel Vetting Guidelines are the following standards:

- **Federal Personnel Vetting Investigative Standards**
- **Common Principles for Applying Federal Personnel Vetting Adjudicative Standards**
- **Federal Personnel Vetting Management Standards**

FEDERAL PERSONNEL VETTING INVESTIGATIVE STANDARDS

The Federal Personnel Vetting Process includes an investigative model aligned to ensure 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. While each vetting domain has its own specific adjudicative criteria, there is a common concern to ensure all trusted insiders demonstrate the following attributes:

- 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 EA 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 nine appendices.

Federal Personnel Vetting Investigative Standards

- Create a risk management approach to investigations that maximizes uniformity across all four Federal Personnel Vetting domains.
- Focus information collection of the most relevant sources, putting less emphasis on seeking specific numbers of each type of source.
- Include a description of the three investigative tiers and the five vetting scenarios.

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 are the Common Principles in Applying Federal Personnel Vetting Adjudicative Standards. The EAs issued these standards in July 2022. Under the Common Principles for Applying 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.

Common Principles in Applying Federal Personnel Vetting Adjudicative Standards

Describes the principles that are common across the four domains of suitability, fitness, national security, and credentialing. Introduces the *whole person concept* which 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: 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 to hold a sensitive position.

5 CFR Part 731: Suitability and Fitness

Establishes and maintains OPM's policies and procedures governing suitability investigations, adjudications, and continuous vetting requirements including the procedures for taking and appealing suitability actions.

5 CFR 737: Credentialing

Determines eligibility for PIV credentials under HSPD-12 including adjudicative standards, requirements for suspension or revocation of eligibility, and reporting requirements for PIV credentialing determinations to the government-wide central repository.

FEDERAL PERSONNEL VETTING MANAGEMENT STANDARDS

The third standard that is at the Operational level under the FPV Guidelines is the Federal Personnel Vetting Management Standards and under these standards are three appendices.

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.

The appendices 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.

Federal Personnel Vetting Management Standards

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.

Appendix A

Personnel Vetting Business Functions

Appendix B

Security Awareness

Appendix C

Reporting Requirements for the Trusted Workforce

FEDERAL PERSONNEL VETTING ENGAGEMENT GUIDELINES

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 PV questionnaires (PVQ) 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 security practitioners implement to support individuals through the vetting process.

Standard Forms

SF-85:
Questionnaire for Non-Sensitive Positions

SF-85P:
Questionnaire for Public Trust Positions

SF-86:
Questionnaire for National Security Positions

TW 2.0

PVQ:
Personnel Vetting Questionnaire (PVQ) in an electronic application (eApp)

FEDERAL PERSONNEL VETTING PERFORMANCE MANAGEMENT GUIDELINES

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.

FEDERAL PERSONNEL VETTING PERFORMANCE MANAGEMENT STANDARDS

To determine the success and needs of PV programs, EAs and D/As collect various types of data as established in the 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

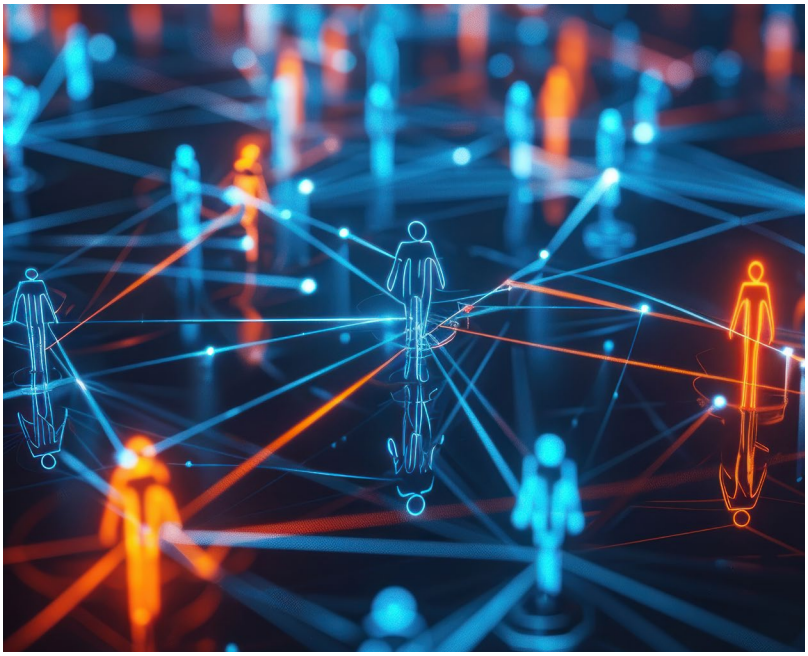
At the operational level, the standards and its appendices establish the minimum measures used to quantify the success of Federal Personnel Vetting programs across the enterprise.

Apendix A:

Performance Metrics

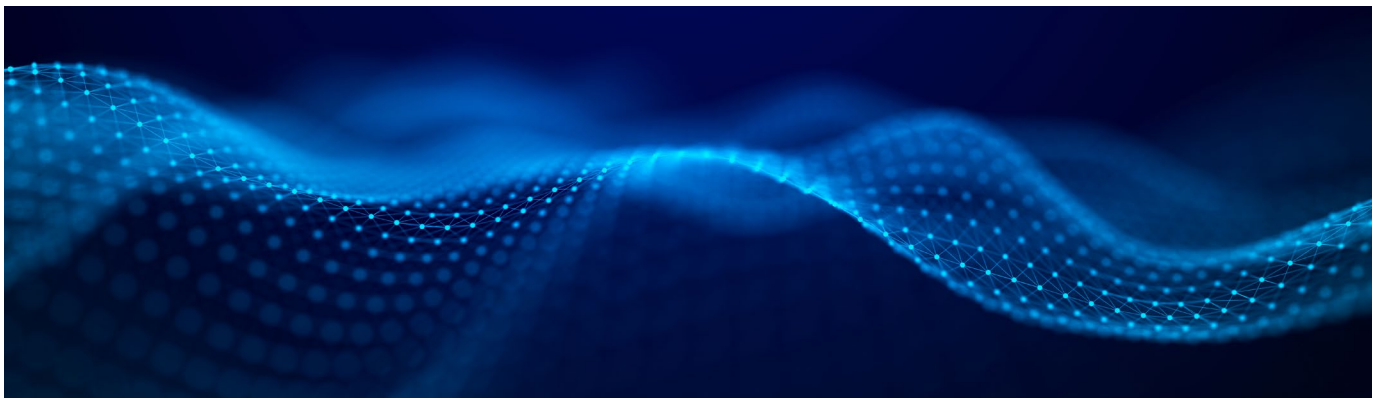
Apendix B:

Quality Management Programs



FEDERAL PERSONNEL VETTING POLICY REVIEW

STRATEGIC LEVEL	TW 2.0 FEDERAL PERSONNEL VETTING CORE DOCTRINE	The Core Doctrine provides the philosophy, goals, and priorities for all PV policy.
GUIDELINES LEVEL	• FEDERAL PERSONNEL VETTING GUIDELINES • PERFORMANCE MANAGEMENT GUIDELINES • PV ENGAGEMENT GUIDELINES	Derived from the Core Doctrine, Guidelines provide high-level strategic direction and outcomes for the PV program. They show how the Core Doctrine is applied.
OPERATIONAL LEVEL	• STANDARDS • STANDARD FORMS	The standards establish the compliance requirements and principles.
TACTICAL LEVEL	• APPENDICES • SEAD 4, 5 CFR PART 731, 5 CFR PART 737	Appendices and other documents contain detailed information and requirements that implement the standards.

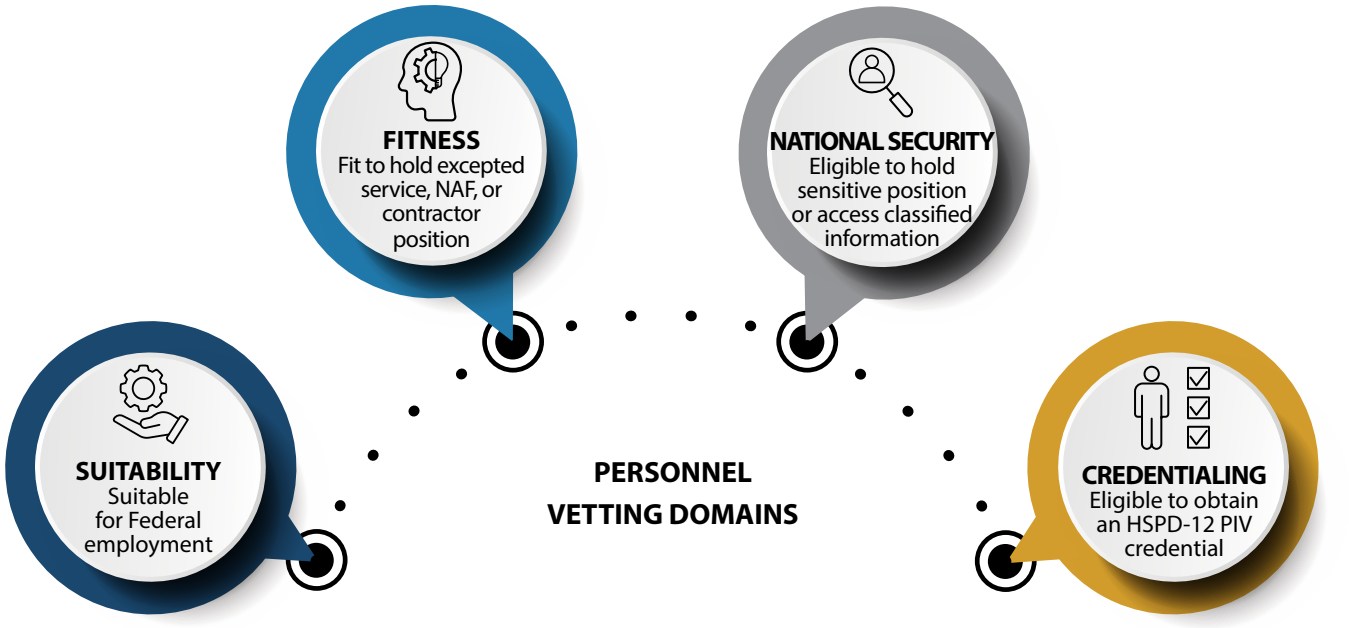


LESSON 4: PERSONNEL VETTING DOMAINS AND FEDERAL PERSONNEL VETTING INVESTIGATIVE STANDARDS

This lesson takes a closer look at the Federal Personnel Vetting Program Framework including the PV domains, attributes of a trusted insider, the three-tier investigative framework, and the five vetting scenarios.

PERSONNEL VETTING DOMAINS

Federal Personnel Vetting is the process by which trusted government personnel evaluate reliable and relevant information from background investigations and other reliable sources to make trust determinations. The process is organized into four domains, each describing the traits and characteristics required for different position requirements and types of access. The adjudicative process culminates in a trust determination or any individual subject to personnel vetting.



SUITABILITY

Suitability refers to a determination of whether the character or conduct of an individual applying to or occupying a position in the competitive service, a position in the excepted service that can-not competitively convert to competitive service, or a career appointment to the Senior Executive Service may have an adverse impact on the integrity or the efficiency of the service.

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

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

FITNESS

Fitness refers to determinations of whether individuals level of character and conduct are fit to work for, or on behalf of, a Federal agency in excepted service positions, Non-Appropriated Fund (NAF) positions, or as defense contractors are suitable to hold those positions.

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

The adjudicative process framework considers the suitability and fitness factors and additional considerations; and culminates in a Fitness trust determination.

NATIONAL SECURITY

National Security refers to a determination of whether an individual's eligibity for access to classifed information or eligibility to hold a sensitive position is clearly consistent with the national security interest of the United States. Any doubt 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 Adjudication Guidelines and the additional factors; and culminates in a National security trust determination.

CREDENTIALING

Credentialing refers to a determination of whether an individual's eligibility to obtain a HSPD-12 compliant PIV credential is consistent with protecting the life, safety, property, or health of individuals with access to Federal faciltiies and with protecting the Government's physical assets or information systems. 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.

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

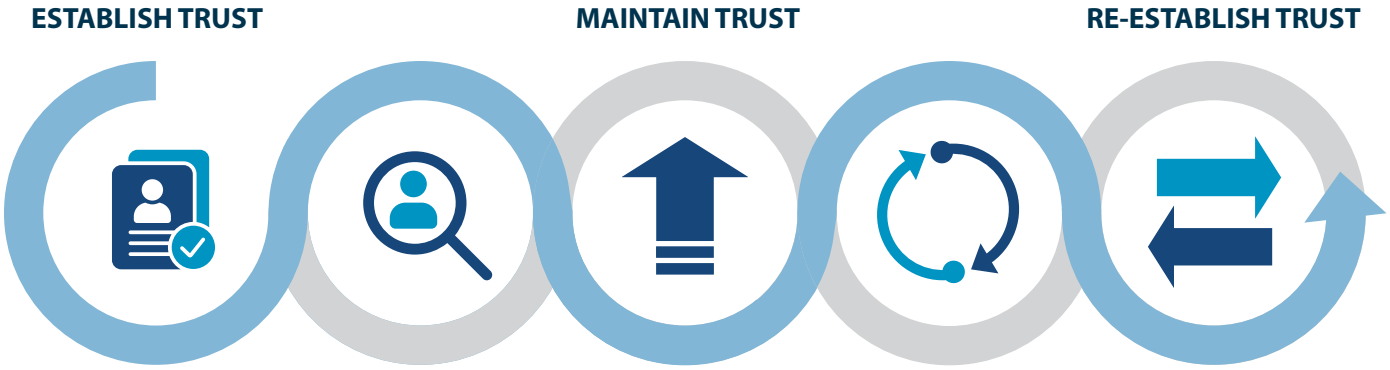
THREE-TIER INVESTIGATIVE MODEL

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

FIVE-TIER MODEL		TW 2.0 FEDERAL PERSONNEL VETTING INVESTIGATIVE STANDARDS THREE-TIER MODEL		
Tier 1	• Low Risk • Non-sensitive • Physical and Logical Access (HSPD-12) credentialing	**Low Tier (LT)**	• Low Risk • Non-sensitive • Physical and Logical Access (HSPD-12) credentialing	Minimum investigation for physical/logical access Access (HSPD-12) credentialing
Tier 2	Moderate-risk public trust	**Moderate Tier (MT)**	Non-sensitive/moderate risk public trust	No National security sensitivity
Tier 3	• Non-critical sensitive • Secret/Confidential • L-Access		Non-critical sensitive/ moderate-risk	• Eligibility for access to Confidential/Secret information • Eligibilty for L-access
Tier 4	High-risk public risk	**High Tier (HT)**	Non-sensitive/high-risk public trust	No National security sensitivity
Tier 5	• Critical-sensitive • Special-sensitive • Top Secret • Sensitive Compartmental Information (SCI) • Q-access		• Critical-sensitive/high-risk • Special-sensitive/high-risk	• Eligibility forTop Secret information • Eligibilty for access to SCI • Eligibility for Q-access

PERSONNEL VETTING SCENARIOS

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. The Federal Personnel Vetting Investigative Standards map the investigative requirements in each scenario which are 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.



INITIAL VETTING

Conducts the initial vetting needed to establish trust with a new individual

CONTINUOUS VETTING

Assesses risk in near real-time to provide insight into trusted insider behavior

UPGRADE

Quickly raises the level of vetting when an individual requires a higher level of trust

TRANSFER OF TRUST

Streamlines movement of trusted individuals between agencies and organizations

RE-ESTABLISHMENT OF TRUST

Simplifies the re-entry of trusted insiders back into the workforce after a period away from government work

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 and is based upon the investigative tier for the position designation.

During initial vetting:

- 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.

CONTINUOUS VETTING

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.

This PV scenario:

- Assesses risk in near real-time.
- Provides insight into trusted inside 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 required to meet the new investigative tier.

TRANSFER OF TRUST

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

- 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.

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

RE-ESTABLISHMENT OF TRUST

The Re-establishment of Trust (RoT) process applies when former trusted insiders who 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.

This PV 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 a break in service
  - Individual's prior PV record

LESSON 5: CONCLUSION

RESOURCES

- Introduction to Federal Personnel Vetting Policy for Security Practitioners Student Guide
- Personnel Vetting Page, CDSE website