Introduction to National Security for Security Practitioners

Elements of Federal Personnel Vetting Job Aid

September 2025

Center for Development of Security Excellence

Contents

Elements of Federal Personnel Vetting Job Aid

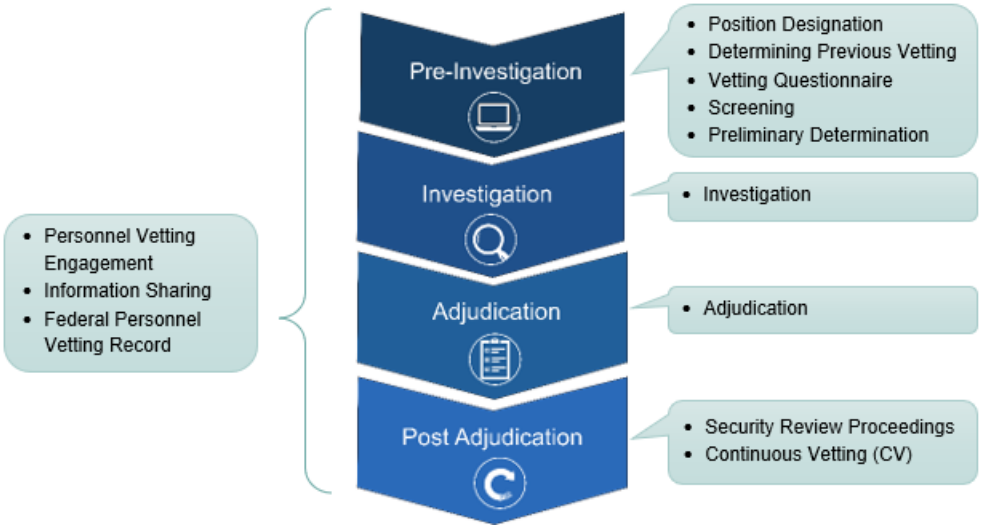
This job aid provides an overview of the 12 elements of Federal personnel vetting identified in the Federal Personnel Vetting Guidelines policy. It also describes the systems commonly used and the policies followed during Federal personnel vetting for national security eligibility.

Elements of Federal Personnel Vetting

National Security Eligibility and the Personnel Vetting Process

National security eligibility determines eligibility for access to classified information or eligibility to hold a sensitive position, to include access to sensitive compartmented information (SCI), restricted data (RD), and controlled or special access program (SAP) information.

Determining an individual's national security eligibility includes 12 elements that can be organized within four main process stages of the Federal personnel vetting process: Pre-Investigation, Investigation, Adjudication, and Post Adjudication. While certain elements apply to specific stages, others are relevant across all stages of the process.



Pre-Investigation

Pre-investigation is the first phase of the Federal personnel vetting process. The pre-investigation phase includes five elements of Federal personnel vetting: Position Designation, Determining Previous Vetting, Vetting Questionnaire, Screening, and Preliminary Determination.

Element	Key Points
Position Designation	• National security positions are any position in a department or agency, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security. • Position sensitivity and risk levels must be designated based on the degree of potential damage to the national security (sensitivity level) and the position's potential for adverse impact to the efficiency or integrity of the service (risk level). National security position designations are: o Critical-Sensitive/High-Risk Public Trust o Special-Sensitive/High-Risk Public Trust o Non-Critical Sensitive/Moderate-Risk Public Trust • The Position Designation System (PDS) helps agency users assess the position's duties and responsibilities to determine the associated sensitivity and risk of the position. The results of the assessment determine: o Risk and sensitivity of the position o Level of investigation needed o Applicable vetting questionnaire required
Determining Previous Vetting	• Departments and Agencies (D/As) security practitioners must review Government-wide high- and low-side record repositories to determine if an individual had been previously vetted. • If an individual has been previously vetted, D/As must review whether the prior level of personnel vetting meets or exceeds the investigative requirements of the position and determine what, if any, additional personnel vetting is required. • There are five Federal personnel vetting scenarios that follow the lifecycle of an individual working for or on behalf of the Federal government and include: o Initial Vetting: Conducts the vetting needed to establish trust with an individual who has not been previously vetted. o Continuous Vetting: Assesses risk in near real-time to provide insight into trusted insider behavior. o Upgrades: Quickly raises the level of vetting when an individual requires a higher level of trust than previously vetted. o Transfer of Trust: Streamlines movement of trusted individuals between agencies and organizations. o Re-establishment of Trust: Simplifies the re-entry of trusted insiders back into the workforce after a break-in-service from government work. • It is important to recognize which of the vetting scenarios applies because the investigative requirements vary by personnel vetting scenario and position designation.

Vetting Questionnaire	• An initial collection of relevant background information by the individual is required using the Standard Form (SF) or Personnel Vetting Questionnaire (PVQ) as applicable. This information, together with relevant investigative information, is used to render national security trust determinations or adjudicative decisions. • Information collected from the Personnel Vetting Questionnaire (PVQ), and predecessor Standard Form SF 86, are used in conducting personnel vetting investigations for national security. (Under Trusted Workforce 2.0, the PVQ parts A, B, and C will replace the SF-86 implemented in eApp.)

Screening	• Screening involves the review of information available to the D/A through the application, hiring, and vetting process to identify information of potential adjudicative concern.
	• D/A's security practitioners may conduct screening prior to an investigation and up to the point of receiving high yield checks (HYCs) through the investigative process.
	• Individuals may receive:
	  ○ An unfavorable screening. D/A may act upon information of potential adjudicative concern, in accordance with applicable laws, regulations, and policies.
	  ○ A favorable screening. A favorable screening does not remove the agency's obligation to make a national security trust determination after the background investigation is complete.

Preliminary Determination	• A preliminary determination is an internal D/A decision based on automated high-yield checks conducted during the initial vetting process. It allows an individual to enter on duty before the completion of the required level of investigation. • For national security sensitive positions, D/A security practitioners may grant temporary eligibility for access to classified information or to occupy the sensitive position upon completion of the high-yield checks per Security Executive Agent Directive (SEAD) 8, Temporary Eligibility.

Investigation

Investigation is the second phase of the Federal personnel vetting process. During this phase, information is gathered on the individual containing both positive and negative information for an assessment against the characteristics of a trusted person to enable a risk-managed trust determination.

Element	Key Points
Investigation	• Executive Order 10450 requires a background investigation for all civilian officers and employees in government departments and agencies. • The scope of the investigation varies based on the position designation. Federal Personnel Vetting Investigative Standards define a three-tier model: Low Tier, Moderate Tier, and High Tier. • The three-tiered model will replace the five-tiered investigative model once fully implemented under TW 2.0 initiative. • The three-tier investigative model uses various information sources, including database checks, written inquiries, interviews, and records. • At the conclusion of the investigation, Investigative Service Providers (ISPs) deliver a Report of Investigation (ROI) to the requesting agency to support trust determinations.

Adjudication

Adjudication is the third phase of the Federal personnel vetting process. During this phase, adjudicators use national security adjudicative guidelines and adjudicative factors to render a national security trust determination.

Element	Key Points

Adjudication	• Adjudication is the key step in determining whether an individual poses an unacceptable risk to national security.
	• When making national security trust determinations, adjudicators use the whole-person concept and guidance from SEAD 4:
	  ○ Thirteen National Security Adjudicative Guidelines, each outlining the security concern, disqualifying, and mitigating conditions.
	  ○ Nine adjudicative factors to evaluate the relevance of an individual's conduct.
	  ○ Six additional factors are applied when information of security concern arises about trusted insiders or individuals who are currently eligible for access to classified information or eligible to hold a sensitive position.
	• Adjudicators must record final trust determinations, favorable and unfavorable, in the applicable government-wide repository.

Post Adjudication

Post Adjudication is the final phase of the Federal personnel vetting process. It encompasses an individual's right to participate in Security Review Proceedings (SRP), formerly known as Due Process and Appeals, and initiates the Continuous Vetting process that ensures ongoing eligibility for the trusted workforce.

Element	Key Points
Security Review Proceedings	• Security Review Proceedings is an administrative process ensuring fair and impartial adjudication when an unfavorable national security eligibility is being considered. • Before an unfavorable determination, individuals must receive specific notifications, have the opportunity to be heard prior to the denial or revocation determination, and the opportunity to appeal the determination.
Continuous Vetting (CV)	• Continuous Vetting (CV) replaces the traditional model of 5- and 10- year periodic reinvestigations. • D/As must enroll each individual in the appropriate CV capability for the corresponding investigative tier and position designation. • The CV level, based on position designation, determines the conditions, information categories, and frequency of vetting to mitigate risk and maintain trust. • Trusted insiders remain enrolled in continuous vetting throughout their Federal service.

Elements of Federal Personnel Vetting that Span the Vetting Process

Three Elements of Federal Personnel Vetting – Federal Personnel Vetting Record, Personnel Vetting Engagement, and Information Sharing– span the entire Federal personnel vetting process. Each of these elements contributes to improved transparency, efficiency, and information sharing.

Element	Key Points
Federal Personnel Vetting Record	• The Federal personnel vetting record includes all personnel vetting-related information for an individual such as vetting determinations, investigations, and adjudicative information. • It is maintained in the government-wide repositories and the D/A internal systems of records.
Personnel Vetting Engagement	• Personnel Vetting Engagement ensures two-way communication between the individual and the Government at all appropriate points in the process.
Information Sharing	• Information sharing, as permitted by law, relies on sharing validated relevant information across and within agencies to eliminate unnecessary duplication and reduce waste. It enhances transparency of the process, ensures quality, and maximizes efficiency while safeguarding and handling sources and methods, protecting privacy, and ensuring fair, consistent treatment for all individuals.

Systems Used in Federal Personnel Vetting

Listed in the following tables are the information systems that support the elements of the Federal Personnel Vetting Process for national security.

System	Description
National Background Investigation Services (NBIS)	• NBIS, once fully implemented, will be the federal government's one-stop-shop IT system for end-to-end personnel vetting – from initiation and application to background investigation, adjudication, and continuous vetting
Pre-investigation Systems	Position Designation Tool (PDT) • Used to designate risk and sensitivity for all positions Electronic Application (eApp) • A portion of the new NBIS system that contains the investigative Standard Form (SF) used by federal applicants and employees to provide information for personnel background investigations

Government-wide Low-side Repository	Central Verification System (CVS)
	• Stores information on investigations and adjudications
	• Searched during the pre-investigation phase for prior investigations and debarments
	Personnel Investigations Processing System (PIPS)
	• Manages the case intake process from electronic application (eApp) through scheduling, closure, and agency delivery
	• Maintains the Security/Suitability Investigations Index (SII), a centralized database of investigations by DCSA and authorized investigative agencies
	• Allows agencies direct access to investigation information
	• Allows agencies to monitor case progress and submit adjudicative decisions
	New Public Portal (NP2)
	• This system provides DCSA customers with the capability for:
	  ○ Secure communication
	  ○ Access to eApp, PIPS, CVS
	  ○ Access to agency-level libraries of investigative notices and other key information, such as continuous vetting alert reports

System	Description
DOD Centralized Low-side Repository	Defense Civilian Personnel Data System (DCPDS) • A human resources information support system for civilian personnel operations in the DOD • System captures position information including position risk and sensitivity Defense Information System for Security (DISS) • DISS is the DOD system of record for national security, suitability, fitness, and credential management for all DOD employees, military personnel, civilians, and DOD contractors • It provides secure communications among adjudicators, security practitioners, and component adjudicators for all personnel categories—military, civilian, and contractor • Component security practitioners use DISS Joint Verification System (JVS) while adjudicators use DISS Case Adjudication Tracking System (CATS) • Under TW 2.0, DISS JVS (a Low-Side Repository) and DISS CATS, (Adjudication Management Platform) will be part of DCSA NBIS IT system
High-side Repository	• The High-Side Repository is a suite of capabilities that provides a government-wide personnel vetting data repository to verify national security sensitive eligibility, access to sensitive compartment information and other controlled access programs, and documented exceptions • The legacy equivalent product is Scattered Castles. Under TW 2.0 capabilities, High-Side Repository will include Transparency of Reciprocity System, or ToRIS

National Security Policy Documents

Listed below are key policies for Federal Personnel Vetting related to national security.

Executive Orders

The Personnel Vetting Program is governed by several executive orders, or E.O.s.

- E.O. 10450: Security Requirements for Government Employment (Apr. 27, 1953)
- E.O. 10865: Safeguarding Classified Information within Industry (Feb. 20, 1960)
- E.O. 12968, as amended: Access to Classified Information (Aug. 2, 1995)
- 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 (Jun. 30, 2008)

- E.O. 13764: Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters (Jan. 17, 2017)
- E.O. 13869: Transferring Responsibility for Background Investigations to the Department of Defense (Apr. 24, 2019)

Security Executive Agency Directive (SEAD)

SEADs are a series of directives from the Office of the Director of National Intelligence (ODNI) in the role of the Security Executive Agent (SecEA). They outline key aspects of the vetting process for national security.

- SEAD 2, Use of Polygraph in Support of Personnel Security Determinations for Initial or Continued Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position (Revised Sep. 1, 2020)
- SEAD 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position (Jun. 12, 2017)
- SEAD 4, National Security Adjudicative Guidelines (Jun. 8, 2017)
- SEAD 5, Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications (May 12, 2016)
- SEAD 6, Continuous Evaluation (CE) (Jan. 12, 2018)
- SEAD 7, Reciprocity of Background Investigations and National Security Adjudications (Nov. 9, 2018)
- SEAD 8, Temporary Eligibility (May 18, 2020)
- SEAD 9, Whistleblower Protection: Appellate Review of Retaliation Regarding Security Clearances and Access Determinations (May 28, 2022)

Intelligence Community Directive (ICD) and Intelligence Community Policy Guidance (ICPG)

An ICD is a policy document issued by the Director of National Intelligence (DNI) that provides formal guidance and requirements for the United States Intelligence Community (IC).

- ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (Oct 2008, Amended June 2018)

ICPG is a supplementary policy document that provides detailed implementation instructions for Intelligence Community Standards (ICS).

- ICPG 704.1, Personnel Security Investigative Standards and Procedures for Access to SCI (Oct 2008, Amended June 2018)
- ICPG 704.3, Denial or Revocation of Access to SCI, Other Controlled Access Program Information, and Appeals Processes (October 2008)
- ICPG 704.4, Reciprocity of Personnel Security Clearance and Access Determinations (Oct 2008, Amended April 2022)
- ICPG 704.5, Intelligence Community Personnel Security Database Scattered Castles (Oct 2008, Revised February 2020)
- ICPG 704.6, Conduct of Polygraph Examinations for Personnel Security Vetting (February 2015)