

What are Some IT Systems Used During Initial Vetting?

Security practitioners use various tools and record repositories to collect and share information, determine previous vetting, and record investigative findings and trust determinations.

Vetting Tools:

- Position Designation Tool (PDT)—Determines a position's risk (impact on the efficiency or integrity of the service) and sensitivity (potential material adverse impact to national security).
- Electronic Application (eApp and eApp-T)—Automates the application process and contains the investigative Standard Forms (SFs) where individuals enter their background information. Referred to as the Personnel Vetting Questionnaire (PVQ).

Low-Side Repository:

- Provides a Government-wide PV record/data repository, on the unclassified domain, to verify:
 - Suitability, credentialing, and national security eligibility and access
 - Trust determinations, investigations, and CV status
- DCSA customer agencies can conduct post-appointment individual management services, and view exceptions.
- National Background Investigation Service (NBIS) Agency—Allows security managers (SSO/FSO) to process background applications and manage them through the investigations' process.
- Investigation Management Platform—Supports the investigation functions of the

five vetting scenarios when performed by a delegated ISP.

- Adjudication Management Platform—Supports conducting and managing adjudicative activities, appeals management, and secure communication between adjudicators and security managers.
- Personnel Vetting Management Platform—Assists agencies in managing PV activities for their workforce such as reporting requirements, administrative actions, visit requests, security incidents, or security awareness briefings.

High-Side Repository:

- Provides a Government-wide PV record/data repository, on the classified domain, to verify:
 - National security eligibility and access
 - Sensitive Compartmented Information (SCI) access, controlled program access, trust determinations, investigations, and CV status
- Intelligence Community (IC) agencies can conduct post-appointment individual management services, and view exceptions.

PERSONNEL VETTING SCENARIOS INITIAL VETTING



For more information, please visit
www.cdse.edu



CDSE

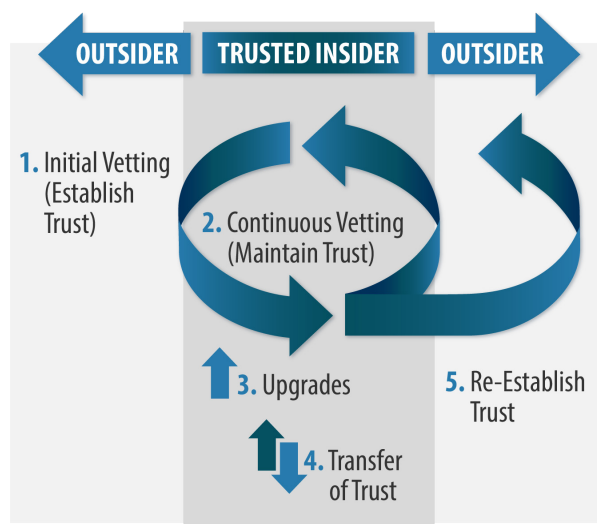
Center for Development
of Security Excellence

Introduction

This job aid provides a high-level overview of the first of the five vetting scenarios, established by the Federal Personnel Vetting Investigative Standards and the Trusted Workforce 2.0 (TW 2.0) initiative.

What is Personnel Vetting?

Personnel Vetting (PV) is the process by which individuals undergo investigation, evaluation, and adjudication to determine whether they should be a trusted insider.



What is Initial Vetting?

- Initial vetting is the first of five PV scenarios and the first step for an outsider to become a trusted insider.
- Establishes a trust relationship between the Government and individuals with the goal of protecting people, property, information, and mission.
- Culminates in a trust determination or adjudicative decision for each PV domain—Suitability, Fitness, National Security, and Credentialing.

How is the Initial Vetting Process Completed?

- Through the application of the central elements or activities performed throughout the PV process.
- Agency component security practitioners start the initial vetting process by identifying the position designation, required investigation type, appropriate vetting questionnaire, and fingerprint requirements.
- Security practitioners screen the required vetting forms and may render a preliminary determination upon results of the high-yield checks (HYC), before the investigation is completed.
- During the vetting process, security practitioners review and enter findings and determinations in the Federal Personnel Vetting Record, engage with individuals, and share information with other agencies as appropriate.
- After the investigation is conducted, the adjudicative authority renders a final trust determination.
 - If favorable, the individual receives the appropriate eligibility and/or access commensurate to the position designation.

- If unfavorable, the individual is afforded security review proceedings (SRP) formerly referred to as due process and appeals for the appropriate PV domain.

Who is a Part of the Initial Vetting Process?

- Security Manager:** Assists and manages individuals through the end-to-end vetting process. Serves as the individual's primary point of contact.
- Investigative Service Provider (ISP):** Conducts the background investigation at the appropriate investigative tier for the individual's position designation and provides a report of investigation (ROI) to the adjudicative authority.
- Adjudicator:** Renders final trust determinations by applying a standard set of guidelines to individuals' specific circumstances, assessing their loyalty, trustworthiness, and reliability, and determining if they are an acceptable risk to protecting people, property, information, and mission.
- Individual:** Completes the required vetting questionnaire and provides additional information as requested during the investigation, adjudication, and continuous vetting (CV).

