

Personnel Vetting Basics

How the US government determines the trustworthiness of its workforce



Why personnel vetting?

The Executive Branch carries out a range of functions on behalf of American people. Agencies rely on their workforces—including military servicemembers, federal employees, and contractors—to meet their strategic goals. Personnel hired to support these agencies are frequently granted access to information systems, facilities, equipment, and sensitive data to perform their duties. This requires agencies to trust that any individuals working on their behalf will use their access responsibly and only in the interest of the American public. Before being granted access, workers undergo federal **personnel vetting**. This is the term for a rules-based set of policies, processes, and tools used to make and maintain a **trust determination**.

How is the level decided?

Agencies choose the level of personnel vetting needed for a position by assessing two related factors: **risk** and **sensitivity**. This categorization—known as a **position designation**—gauges how much damage someone in the position could do. The greater the potential for harm associated with the position, the higher level of vetting required. Both government and contractor job announcements typically indicate the level of personnel vetting required for each position.

Position Designations

Agencies are **required** to assess the **risk** of jobs within the context of how the position could affect the **public's trust** in their government, if abused. There are three categories simplified below.

- **Low Risk** - Could do some harm or discernable damage to the public's trust.
- **Moderate Risk** - Could produce fair amount of harm or serious damage to the public's trust.
- **High Risk** - Could produce substantial degree of harm or serious damage to the public's trust.

When assessing a position's **sensitivity**, an agency assesses to extent the position could cause damage to **national security** if abused. It uses three categories of sensitivity **defined** in regulation and simplified below.

- **Noncritical-Sensitive** - Significant or serious damage
- **Critical-Sensitive** - Exceptionally grave damage
- **Special-Sensitive** - Inestimable damage

"Critical-Sensitive" and "Special-Sensitive" are by default High Risk positions. However, "Noncritical-Sensitive" positions can be High Risk or Moderate Risk.

Jobs with no impact on national security are categorized as "Non-Sensitive" and can be any risk level.

What are the different types of vetting decisions?

All trust determinations focus on evaluating common characteristics of a trusted individual: good conduct, integrity, sound judgment, loyalty, and reliability. These decisions types—called **vetting domains**—address distinct aspects of trustworthiness as explained below. Most positions require a worker to be successfully vetted across multiple vetting domains.



Suitability/Fitness

Determines whether an individual should be trusted to perform relevant job functions. The terms "suitability" and "fitness" are similar concepts that apply to different categories of positions.

- Often called **Public Trust** vetting.
- Required for almost all positions, including national security positions.
- Focused on whether the individual obeys laws, follows workplace rules, and demonstrates loyalty to United States.



Credentialing

Determines whether an individual should be trusted with access to government facilities, personnel, and/or information technology systems. Needed for most positions.

- Meets ID requirement from [HSPD-12](#).
- Authorizes a Personal Identity Verification (PIV) card for civilian agencies or Common Access Card (CAC) for the Department of Defense.
- Minimum vetting for small segment of positions outside national security and suitability/fitness domains.



National Security

Determines whether an individual should be trusted in a position that could materially affect national security, with or without access to classified information. Includes all security clearance levels and supplemental accesses such as-

- Sensitive Compartmented Information (SCI).
- Special Access Programs (SAPs).
- "Q" / "L" accesses related to the development, production, and use of nuclear weapons.

How do position designations affect investigations?

The type of background investigation an individual receives is based on the position designation. Called tiers, these dictate what data will be collected during an investigation. Under ongoing reforms, the number of tiers is being reduced from five to three. Fewer tiers will make it easier for vetted workers to move between agencies, but the transition to three tiers will take several years to complete. The table below indicates investigative tier required by position designation for both the legacy and reformed models.

Position Designation & Possible Applications	Legacy Tier	New Tier
Non-Sensitive / Low Risk (<i>Low Risk</i>)	1	Low
Non-Sensitive / Moderate Risk (<i>Public Trust – Moderate Risk</i>)	2	Moderate
Non-Critical Sensitive / Moderate Risk (<i>Secret, Confidential, & "L" access</i>)	3	
Non-Sensitive / High Risk (<i>Public Trust – High Risk</i>)	4	High
Critical Sensitive / High Risk Special Sensitive / High Risk (<i>Top Secret, SCI, "Q" access, & most SAPs</i>)	5	

Additional Screening

Some jobs require the individual to undergo medical, psychological, or polygraph evaluations during the vetting process.

Called "enhanced" vetting, these requirements often apply to jobs within the [Intelligence Community](#) or law enforcement agencies.

The average time to make a trust determination is much longer for positions requiring these additional assessments.

What are the steps in the personnel vetting process?

Once a position is designated with a required level of vetting, the hiring agency/company will identify a candidate for the job. This is the point where individuals begin engaging the personnel vetting process. Specific elements of the process can vary based on the position and hiring process, but the fundamentals are the same.

1

Forms Completion

Once an agency or contractor extends an individual a "conditional" or "tentative" employment offer—unless they already hold an equal or higher trust determination—they will be asked to provide fingerprints and complete electronic forms. This will include a questionnaire used to collect personal data—such as places lived, employment history, foreign travel, and close associates—needed to conduct the background investigation.

2

Background Investigation

Specially-trained investigators will verify the information provided in the questionnaire, clarifying any missing or inaccurate data. They may also interview the individual being investigated and anyone who knows them well. All relevant data will be consolidated in a "report of investigation".

3

Trust Determination & Access

Once completed, the report of investigation is provided to a trained adjudicator outside of the investigation process to make the trust determination, based on the totality of their behavior. This decision can cover one or more of the vetting domains. Agencies may make a preliminary determination that allows the individual to begin work before the full background investigation is complete and a final trust determination is made.

4

Continuous Vetting

After determining trustworthiness, agencies still need to know if any new information emerges that could lead the government to reconsider its decision. Most positions are enrolled into a service called continuous vetting that routinely checks for new information that could affect the agency's trust determination.

Classified Data: Eligibility vs. Access

Most Americans are familiar with "classified" information—also sometimes called national security information—due to its prevalence in popular culture. Covering a [range of topics](#), it is defined as data that would harm the United States if disclosed to adversaries. It is important that any worker who may need access be thoroughly vetted considering the consequences of unauthorized disclosure. A common risk mitigation approach is for the government to minimize how many people can view that data. Consequently, some individuals vetted for a sensitive position are given national security **eligibility** without being granted **access** until their agency decides they need the information to perform their duties.