A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A	

Back to Top

B	
Background Investigation (BI)	Scrutiny of applicants to work for or on behalf of the Federal Government by process of collecting and verifying information about an individual's past and present to assess their loyalty, judgement, character, and reliability.

Back to Top

C	
Center for Development of Security Excellence (CDSE)	A directorate within the Defense Counterintelligence and Security Agency (DCSA) that provides security education, training, and certification products and services.
Central Verification System (CVS)	Central data repository for viewing and recording information on existing security eligibilities, background investigations, suitability, fitness, and Homeland Security Presidential Directive (HSPD)-12 determinations that enables reciprocity among Federal agencies.
Code of Federal Regulation (CFR)	See Federal regulation.
Common Access Card (CAC)	An identification within Department of Defense (DOD) that serves as the Personal Identity Verification (PIV) Card required by Homeland Security Presidential Directive (HSPD)-12 and its implementing guidance.
Common Principles for Applying Federal Personnel Vetting Adjudicative Standards	A document at the Operational level of the Federal Personnel Vetting Policy Framework and that falls under the Federal PV Guidelines that describe the principles that are common across the four domains and introduce the whole person concept that should be considered in reaching a national security eligibility determination.
Continuous Evaluation (CE)	Vetting process to review the background of an individual determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to assist in the ongoing assessment of an individual's continued eligibility. CE is intended to complement continuous vetting efforts.
Continuous Vetting (CV)	Robust and near real-time review of the background of trusted individuals at any time during their Government affiliation to determine whether they continue to protect people, property, information, and mission.
Credentialing	The process that determines who may receive Personal Identity Verification (PIV) credentials for physical access to Federal-controlled facilities and/or logical access to Federal-controlled information systems.

C	
Critical sensitive	A position sensitivity designation indicating the potential for exceptionally grave impact on national security.

Back to Top

D	
Defense Counterintelligence Security Agency (DCSA)	An agency of the Department of Defense (DOD) that provides investigation and adjudication services to the Federal Government and entities.
Department of Defense (DOD)	A Federal Government agency that is responsible for the military forces.
Department or agency (D/A)	Federal Government offices overseen by the President of the United States and organization within Federal and state governments that are responsible for the oversight and administration of specific sectors or fields.
Director of National Intelligence (DNI)	The head of the United States Intelligence Community (IC) who is appointed by the President and approved by the Senate.

Back to Top

E	
Electronic application (eApp)	An application that has replaced Electronic Questionnaires for Investigations Processing System (e-QIP) as the mechanism by which Federal applicants and employees complete the investigative Standard Forms (SFs) and provide the necessary information to process their personnel background investigations.
Executive Agent (EA)	A Federal agency leadership, usually an agency director, that is responsible for developing, implementing, and overseeing effective, efficient, and uniform policies, procedures, and standards.
Executive Order (E.O.)	A type of presidential issuance that is issued by the President of the United States and direct Federal Government operations.
E.O. 10450 (1953): Security Requirements for Government Employment	A presidential issuance that requires that all persons employed in Government departments and agencies (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	A presidential issuance that 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	A presidential issuance that establishes a uniform Federal personnel security program (PSP) for individuals considered for initial or continued eligibility for access to classified information or eligibility for a sensitive position.

E	
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	A presidential issuance that establishes a personnel vetting (PV) policy and procedures for vetting individuals who work for or on behalf of the Federal Government and requires all executive branch agencies to implement reforms to enhance their personnel security programs (PSPs) and establish a single vetting system for the Federal Government.
E.O. 13488, as amended (2009): Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust	A presidential issuance that establishes reinvestigation requirements for public trust positions and reciprocal acceptance of fitness determinations.
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	A presidential issuance that provides the authorities needed to modernize, strengthen, and ensure a secure, efficient, and timely background investigation process and makes risk-based decisions and addresses evolving threats.
E.O 13869 (2019), Transferring Responsibility for Background Investigations to the Department of Defense	A presidential issuance that transferred National Background Investigations Bureau (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 E.O. 13467.

Back to Top

F	
5 CFR Part 731: Suitability and Fitness	Regulations that govern the personnel vetting (PV) investigative and adjudicative processes for determining suitability and fitness and that is at the Tactical level of the Federal Personnel Vetting Policy Framework, under the Common Principles for Applying Federal Personnel Vetting Adjudicative Standards.
5 CFR Part 732: National Security Positions	Regulations that establish National security investigation and adjudication policy and that is at the Tactical level of the Federal Personnel Vetting Policy Framework, under the Common Principles for Applying Federal Personnel Vetting Adjudicative Standards.
5 CFR Part 736: Personnel Investigations	Regulations that establish the requirements for personnel investigations conducted by the Office of Personnel Management (OPM), and for those conducted under delegated authority from OPM.
5 CFR Part 737: Credentialing	Regulations that establish the requirements for determining eligibility for Personal Identification Verification (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	Regulations that establish position designations and investigation requirements.

F	
32 CFR Part 117: National Industrial Security Program Operating Manual (NISPOM)	Regulations that establish requirements for cleared contractors under the National Industrial Security Program (NISP).
5 U.S.C. § 552: Freedom of Information Act (FOIA)	A Federal law that allows individuals to request records from Federal agencies, including types of background checks and processes and contain exemptions for personnel files and other information for national security and law enforcement purposes.
50 U.S.C. § 3341: Security Clearances	A Federal law that establishes the responsibility for direction of investigations and adjudications and reciprocity of trust (RoT) determinations.
Federal law	Also known as statutes or codes, are rules created by the legislative branch of the Government, such as Congress, and signed by the President that define how people should behave in areas that are under the authority of the Government to protect citizens rights and ensure their safety.
Federal Personnel Vetting	The process by which individuals undergo investigation, evaluation, and adjudication. It encompasses the policies, processes, and tools used to determine whether personnel should be trusted to work for or on behalf of the Government, to occupy a sensitive position, and/or have access to Government information technology (IT) systems or facilities.
Federal Personnel Vetting Engagement Guidelines	A document at the Guidelines level of the FPV Policy Framework that provide engagement components based on the five personnel vetting scenarios and that security practitioners implement to support individuals through the vetting process.
Federal Personnel Vetting Guidelines	A document at the Guidelines level of the Federal Personnel Vetting Policy Framework that describes the high-level outcomes for the FPV risk management framework, how an individual is assessed against the characteristics of a trusted person, successful outcomes for the five personnel vetting scenarios, and the central elements of FPV.
Federal Personnel Vetting Investigative Standards	A document at the Operational level of the Federal Personnel Vetting Policy Framework and that falls under the FPV Guidelines that create a risk management approach to investigations, focus information collection on obtaining the most relevant sources of information, and include a description of the three investigative tiers and the five personnel vetting scenarios.
Federal Personnel Vetting Investigative Standards Appendices	Nine appendices at the Tactical level of the Federal Personnel Vetting Policy Framework that fall below the FPV Investigative Standards.

F	
Federal Personnel Vetting Management Standards	A document at the Operational level of the Federal Personnel Vetting Policy Framework that falls under the FPV Guidelines that 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.
Federal Personnel Vetting Management Standards Appendices	Three appendices at the Tactical level of the Federal Personnel Vetting Policy Framework that fall below the Federal Personnel Vetting Management Standards.
Federal Personnel Vetting Performance Management Guidelines	A document at the Guidelines level of the Federal Personnel Vetting Policy Framework that provide an overarching direction for a successful FPV 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	A document at the Operational level of the Federal Personnel Vetting Policy Framework that falls under the FPV Performance Management Guidelines that establish the minimum measures used to quantify the success of personnel vetting (PV) programs across the enterprise.
Federal Personnel Vetting Performance Management Standards Appendices	Two appendices at the Tactical level of the Federal Personnel Vetting Policy Framework that fall below the FPV Performance Management Standards.
Federal Personnel Vetting Policy Framework	A suite of policies organized in a top-down hierarchical structure with four levels, where each successive level is more agile that includes a core doctrine, guidelines, standards, standard forms, and appendices.
Federal regulation	Also known as rules, requirements that are created by the executive branch agencies to explain how to implement and interpret laws passed by Congress.
Fitness	The level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency.

Back to Top

G	
Guidelines level	The second of four levels of the Federal PV Policy Framework that contains the Federal PV Guidelines, Federal PV Engagement Guidelines, and Federal PV Performance Management Guidelines.

Back to Top

H	
High tier (HT)	Investigative tier 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 that includes eligibility and access to Top Secret information, Sensitive Compartmented Information (SCI), or Q access.
High risk	A final position designation reflecting the potential for exceptionally serious impact critical to the Department of Defense (DOD) mission or program, or the integrity or efficiency of the service.
Homeland Security Presidential Directive (HSPD)-12: Policy for a Common Identification Standard for Federal Employees and Contractors	A Presidential issuance that establishes a standard badging process for Federal employees and contractors with the intention of enhancing security, reducing identity fraud, and protecting personal privacy and a process that requires credentialing determinations of employees and contractors for access to Government-controlled facilities and information and the issuance of Personal Identity Verification (PIV) cards.

Back to Top

I	
ICD 704: Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information	A directive that implements the Personnel Security Program (PSP) within the Intelligence Community (IC), establishes the policy and procedures for access to Sensitive Compartmented Information (SCI), provides the baseline personnel security standards and exceptions for access to SCI, and authorizes polygraph programs for IC elements.
ICPG 704.1: Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information	A policy guidance that expands on ICD 704 by providing investigative standards for access to SCI and controlled access programs; setting policy for source collection; establishing investigative standards, including coverage, estimates, and time periods; and establishing requirements for training and quality control.
ICPG 704.3: Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes	A policy guidance that mandates that individuals who have been considered for and denied initial or continued access to SCI shall be afforded an opportunity to appeal and establishes a process for all appeals.
ICPG 704.4: Reciprocity of Personnel Security Clearance and Access Determinations	A policy guidance that provides direction on the application of reciprocity, including situations where adjudicative decisions differ between agencies; establishes the Security Executive Agent (SecEA) as the final arbitrative authority between agencies regarding adjudications; and mandates standardized training for investigative and adjudicative personnel.

I	
ICPG 704.5: Intelligence Community Personnel Security Database Scattered Castles	A policy guidance that establishes Scattered Castles, a database that stores personnel security information, as the repository for all eligibility and access determinations and defines the roles and responsibilities for the database's operation and support.
ICPG 704.6: Conduct of Polygraph Examinations for Personnel Security Vetting	A policy guidance that provides direction for authorizing and conducting polygraph examinations and distinguishes policy and requirements for Counterintelligence Scope Polygraphs (CSPs), Expanded Scope Polygraphs (ESPs), and Specific Issue Polygraphs (SIPs).
Information technology (IT)	A field that uses technology to analyze, store, and communicate date information using computers, software, networks, etc.
Initial vetting	Vetting scenario that 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.
Intelligence community (IC)	Various Federal agencies that collect and analyze intelligence and use it to support national security.
Intelligence Community Directive (ICD)	Standard that is established by the Director of National Intelligence (DNI) that provides policy and guidance to the IC that governs operations and functions.
Intelligence Community Policy Guideline (ICPG)	Guideline that dictates how the IC conducts intelligence activities, handles sensitive information, and responds to specific situations, ensuring consistency across the entire intelligence apparatus.
Intelligence Reform and Terrorism Prevention Act of 2004	A law that establishes a single department or agency (D/A) to be responsible for security clearance determinations and investigations, requires all D/As to reciprocally accept background investigations and determinations, and establishes an integrated, secure database on security clearances.

Back to Top

J	

Back to Top

K	

Back to Top

L	
L access	Permits a Department of Energy (DOE) individual to have access, on a need-to-know basis, to Confidential Restricted Data, Secret, and Confidential Formerly Restricted Data, or Secret and Confidential National Security Information, required in the performance of duties, provided such information is not designated classified cryptographic information (CRYPTO), other classified communications security (COMSEC) information, or intelligence information.
Low risk	A final position designation reflecting the potential for limited impact to the Department of Defense (DOD) mission or program, or the integrity or efficiency of the service.
Low tier (LT)	Investigative tier for Non-Sensitive/Low-Risk positions and is the equivalent to the current Tier 1 investigation that is the minimum investigation tier for granting physical and/or logical access to facilities and making credentialing (HSPD-12) determinations.

Back to Top

M	
Moderate risk	A final position designation reflecting the potential for exceptionally serious impact critical to the Department of Defense (DOD) mission or program, or the integrity or efficiency of the service.
Moderate tier (MT)	Investigative tier 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 that includes eligibility and access to Confidential or Secret information, or L access, all align to this tier.

Back to Top

N	
National Industrial Security Program Operating Manual (NISPOM)	A document that establishes requirements for the protection of classified information disclosed to or developed by contractors, licensees, grantees, or certificate holders to prevent unauthorized disclosure. See 5 CFR Part 1400: Designation of National Security Positions.
National Background Investigations Bureau (NBIB)	A Federal Government agency that fell under the Office of Personnel Management (OPM) that was transferred under the Department of Defense (DOD) and became the Defense Counterintelligence and Security Agency (DCSA).

N	
National Industrial Security Program (NISP)	A partnership between the Federal Government and private industry administered by the Defense Counterintelligence and Security Agency (DCSA) to safeguard classified information.
National security domain	The vetting domain in which the individual requires access to classified information or to hold a national security position. Individuals are trustworthy and reliable.
Non-appropriated funds (NAF)	Funds that are not allocated by Congress and are usually generated from the sale of goods or services.
Non-critical sensitive	A position sensitivity designation indicating the potential for moderate to serious impact on national security.
Non-sensitive	A position sensitivity designation indicating there is no potential for impact on national security

Back to Top

O	
Office of the Director of National Intelligence (ODNI)	See Director of National Intelligence.
Office of Personnel Management (OPM)	The chief human resources agency and personnel policy manager for the Federal Government.
One-Three-Five Framework	Components of Federal personnel vetting and Trusted Workforce 2.0 (TW 2.0) that applies across all of the Personnel Vetting Domains and includes: one personnel vetting model, three investigative tiers, and five vetting scenarios.
Operational level	The third of four levels of the Federal Personnel Vetting Policy Framework that includes policies that are compliance oriented and include such tools as standards, principles, and common forms.

Back to Top

P	
People, property, information, and mission (PPIM)	The key assets and elements that the Federal personnel vetting program and trusted insiders are responsible for protecting.
Performance Accountability Council (PAC)	Appointed by the President, a group of individuals that are spearheading personnel vetting reforms under the Trusted Workforce (TW) 2.0 initiative.
Personnel Identity Verification (PIV)	A Federal Government credential used to access federally controlled facilities and information systems at the appropriate security level.
Personnel Security Program (PSP)	A program that establishes the standards, criteria, and guidelines upon which national security personnel security trust determinations are based.
Personnel vetting (PV)	The process in which trusted Government personnel evaluate the reliable and relevant information from background investigations and other reliable sources to make national security, suitability, fitness, and credentialing trust determinations.

P	
Personnel vetting domains	Four types of personnel vetting based upon traits and characteristics required for different position requirements and types of access and includes suitability, fitness, national security, and credentialing. The adjudicative process culminates in a trust determination related to each domain.
Personnel Vetting Model	A component of the One-Three-Five Framework that aligns the vetting processes with a simplified framework of Executive issuances, guidelines, and standards.
Personnel Vetting Questionnaire (PVQ)	A common form developed by the Office of Personnel Management (OPM) that will replace Standard Forms (SFs) 85, 85P, and 86 and will be used to conduct personnel vetting investigations for low risk, public trust, and/or national security positions.
Personnel vetting scenarios	All personnel vetting falls within one of five vetting scenarios depending on the mission need, the relevant circumstances of the individual being vetted, the duties and responsibilities of the position, and the management of human risk.
Position Designation System (PDS)	A Defense Counterintelligence and Security Agency (DSCA) system that assesses the duties and responsibilities of a position to determine if a position's duties and responsibilities have potential for incumbents to bring about a material adverse effect on the national security, and the degree of that potential effect, which establishes the sensitivity level of a position. The results of this assessment determine what level of investigation should be conducted for a position.
Presidential issuance	Executive Orders (E.O.s) and Presidential Policy Directives (PPDs) that are issued by the President of the United States and direct Federal Government operations.
Presidential Policy Directive (PPD)	A type of presidential issuance.
Presidential Policy Directive (PPD) 19 (2012): Whistleblower Protection	A presidential issuance that 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.
Privacy Act of 1974	A law that prohibits Federal agencies from disclosing information about an individual contained in a system of record without the prior written consent of that person, requires maintenance of accurate and complete records, and allows individuals to access their own personnel records.
Public trust	Positions that are of moderate- and high-risk positions that may involve access to, operation of, or control of: policy, programs, IT systems, public safety and health, law enforcement, financial or personal records, or other duties requiring a significant degree of public trust.

Back to Top

Q	
Q access	Permits a Department of Energy (DOE) individual to have access, on a need-to-know basis, to Top Secret, Secret, and Confidential Restricted Data, Formerly Restricted Data, National Security Information, or special nuclear material in Category I or II quantities as required in the performance of duties.

Back to Top

R	
Reciprocity	Recognition of favorable trust determinations when the determination was based on criteria equivalent to standards established by the Office of Personnel Management (OPM).
Re-establishment of trust (RoT)	Personnel vetting scenario that occurs when former trusted insiders who stop performing work for or on behalf of the Federal Government for a period of time, seek to return.

Back to Top

S	
SEAD 1: Security Executive Agent Authorities and Responsibilities	A directive that consolidates and summarizes the authorities and responsibilities of the Security Executive Agent (SecEA) to develop, implement, and oversee policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information or eligibility to hold a sensitive position.
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	A directive that establishes policy and assigns responsibilities governing the use of polygraph examinations conducted by agencies in support of personnel vetting 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	A directive that establishes reporting requirements for all covered individuals who have access to classified information or hold a sensitive position.
SEAD 4: National Security Adjudicative Guidelines	A directive that establishes 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.
SEAD 5: Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations	A directive that provides guidance for the collection, use, and retention of publicly available social media information for initial and continued eligibility for access to classified information or to hold a sensitive position.

S	
SEAD 6: Continuous Evaluation	A directive that establishes policy and requirements to continually monitor individuals in national security positions to ensure they continue to meet eligibility requirements.
SEAD 7: Reciprocity of Background Investigations and National Security Adjudications	A directive that establishes requirements for reciprocal acceptance of background investigations and national security adjudications for initial or continued eligibility for access to classified information or eligibility to hold a sensitive position.
SEAD 8: Temporary Eligibility	A directive that establishes policy and requirements for authorizing temporary eligibility for access to classified information or temporary eligibility to occupy a sensitive position, one-time access or to access information at a higher level.
SEAD 9: Whistleblower Protection: Appellate Review of Retaliation Regarding Security Clearances and Access Determinations	A directive that establishes policy for the Director of National Intelligence's (DNI's) appellate review process for employees who seek to appeal an adverse final agency determination with respect to alleged retaliatory actions taken by an employing agency affecting the employer's security eligibility or access determination as a result of protected disclosures.
Security Executive Agent (SecEA)	The Director of National Security (DNI) and is responsible for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information and eligibility to hold a sensitive position.
Security Executive Agent Directive (SEAD)	Directives issued by the DNI as the Security Executive Agent (SecEA) that 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.
Security Training, Education, and Professional Portal (STEPP)	Center for Development of Security Excellence's (CDSE's) learning portal and learning management system (LMS).
Sensitive compartmented information (SCI)	Highly classified information about certain intelligence sources and methods and can include information pertaining to sensitive collection systems, analytical processing, and targeting, or which is derived from it.
SF 85: Questionnaire for Nonsensitive Positions	A personnel vetting (PV) questionnaire completed by individuals in non-sensitive, low risk positions.
SF 85P: Questionnaire for Public Trust Positions	A PV questionnaire completed by individuals in non-sensitive, moderate risk, and high-risk positions.
SF 86: Questionnaire for National Security Positions	A PV questionnaire completed by individuals in national security positions.

S	
Special Access Program (SAP)	Protocol established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.
Special sensitive	A position designation reflecting the potential for inestimable damage to national security.
Standard Form (SF)	An application, information collection request, or services request document that is numbered and issued by the Federal Government.
Standard Operating Procedure (SOP)	An agency or organization's instructions on how to complete a process or task.
Strategic level	The top level of the Federal Personnel Vetting Policy Framework that contains the Trusted Workforce (TW) 2.0 FPV Core Doctrine and TW 2.0 Executive Correspondences.
Suitability	A person's identifiable character traits and conduct sufficient to decide whether an individual's employment or continued employment would or would not protect the integrity or promote the effectiveness or efficiency of the Federal service.
Suitability and Credentialing Executive Agent (Sec/Cred EA)	The Director of the Office of Personnel Management (OPM) and is responsible for establishing the standards agencies use to evaluate whether an individual is suitable or fit for Federal service.

Back to Top

T	
32 CFR Part 117: National Industrial Security Program Operating Manual (NISPOM)	A rule that establishes requirements for contractors that are security eligible under the National Industrial Security Program (NISP).
Tactical level	The bottom level of the Federal Personnel Vetting Policy Framework that contains appendices and detailed information that are applied in the personnel vetting mission set of duties.
Three-Tier Investigative Model	The three tiers align investigative requirements for suitability, fitness, national security, and credentialing decisions that enable greater workforce mobility while simultaneously reducing duplication and complexity in the investigative process. The model will replace current five-tier Investigative Model.
Title VIII of the National Security Act of 1947	A law that established the requirements for accessing classified information, including background checks, and uniform standards.

T	
Transfer of trust (ToT)	Personnel vetting (PV) scenario that occurs when individuals move from one agency to another and is commonly referred to as reciprocity.
Trust determination	PV domain (suitability, fitness, national security, and credentialing) determinations that found an individual can be trusted to protect people, property, information, and mission (PPIM). Formerly known as adjudication.
Trusted insider	An individual who completed the Federal Personnel Vetting process and was determined trustworthy of people, property, information, and mission (PPIM).
Trusted Workforce 2.0 (TW 2.0)	The vetting reform initiative that 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.
Trusted Workforce 2.0 Executive Correspondences	Documents at the Strategic level of the Federal Personnel Vetting Policy Framework that accompany the Trusted Workforce (TW) 2.0 Federal Personnel Vetting Core Doctrine and contains interim guidance and changes as the policies were developed.
Trusted Workforce 2.0 Federal Personnel Vetting Core Doctrine	A document at the Strategic level of the Federal Personnel Vetting Policy Framework that establishes the philosophy for the Government's PV program and will guide the development of Government-wide and agency policy. It defines the PV mission, its guiding principles, key supporting processes, and policy priorities.
Trusted Workforce 2.0 Transforming Workforce Vetting Charter	A document that was released in 2018 announced and initiated the TW 2.0 initiative.

Back to Top

U	
Upgrades	PV scenario that occurs 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.
United States Code (U.S.C.)	See Federal law.

Back to Top

V

Back to Top

W	
Whole person concept	An adjudication model that stipulates that all available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a trust determination.

Back to Top

X

Back to Top

Y

Back to Top

Z

Back to Top