PERSONNEL VETTING PROGRAM

1. **REASON FOR ISSUE**: This directive provides updated guidance and revised policies for the Department of Veterans Affairs (VA) Personnel Vetting Program.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES**: This directive revises and updates the policy and responsibilities for managing, administering, and implementing the VA Personnel Vetting Program. Major changes include:

   a. Changes the title from Personnel Security and Suitability Program to the Personnel Vetting Program.

   b. Changes the title from Security and Investigation Center to Personnel Security Adjudication Center (PSAC).

   c. Changes the title from National Background Investigation Bureau to Defense Counterintelligence and Security Agency (DCSA).

   d. Allows for Servicing Personnel Vetting Offices to adjudicate employee and affiliate Public Trust (Moderate and High Risk) investigations except for VA Police Officers.

   e. Revises personnel vetting investigative and adjudicative processes for determining suitability and fitness and mandates that the same criteria will be used for making both suitability and fitness determinations.

   f. Eliminates the five-year periodic reinvestigation requirement for public trust positions.

   g. Removes the 24-month break-in-service provision regarding reciprocity.

   h. Establishes a requirement for continuous vetting for all individuals who perform, or who seek to perform, work for the executive branch in competitive service, excepted service, career Senior Executive Service, and contractors.

   i. Mandates use of VA Centralized Adjudication Background Investigation System (VA-CABS) for VA suitability, fitness, and national security adjudications.

3. **RESPONSIBLE OFFICE**: Office of Human Resources and Administration/Operations Security and Preparedness (HRA/OSP) (006), Office of Identity, Credential, and Access Management (OICAM) (07C).

4. **RELATED HANDBOOK**: VA Handbook 0710, Personnel Vetting Program, dated September 08, 2025.

5. **RESCISSION:** VA Directive 0710, Personnel Suitability and Security Program dated June 4, 2010.

Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 0710
Transmittal Sheet
September 08, 2025

CERTIFIED BY:

/s/
Nathan T. Sanfilippo
Acting Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Mark R. Engelbaum
Assistant Secretary for
Human Resources and
Administration/Operations, Security, and
Preparedness

DISTRIBUTION: Electronic Only

TABLE OF CONTENTS

1. PURPOSE. 4

2. POLICY. 4

3. RESPONSIBILITIES 8

4. AUTHORITIES 10

5. REFERENCES 12

6. DEFINITIONS 12

PERSONNEL VETTING PROGRAM

1. PURPOSE.

a. This directive provides strategic direction for the Department of Veterans Affairs' (VA) Personnel Vetting Program (PVP) to ensure a trusted workforce that will protect people, property, information, and mission. The VA's Personnel Vetting Program applies to Federal applicants, appointees, employees, contractors, volunteers, and affiliates who have access to Departmental operations, facilities, information, or information technology systems.

b. The PVP encompasses vetting for suitability, fitness, national security (eligibility for or continued access to classified information or to hold a sensitive position) and issuing a Federal identity credential. Establishing and maintaining trust is a core goal of the Federal Personnel Vetting Program.

c. Effective Government operations require that the Government's workforce be trusted to deliver on mission, provide excellent service, and demonstrate effective stewardship of taxpayer funds.

2. POLICY.

a. **Program Administration.**

(1) VA's Personnel Vetting Program Management Office is authorized to conduct oversight and compliance reviews of the organizations with delegated authority to adjudicate for suitability and fitness. VA Administrations and Staff Offices may issue additional Directives, Handbooks, or policies governing PVP. Any such policies must be in alignment with VA Directive and Handbook 0710 and may be issued only after review and approval by VA Personnel Vetting Program Office.

(2) VA-CABS is the case management system for Personnel Security Specialists to enter position designation records, record background investigation adjudications for suitability and fitness, document and apply reciprocity and manage continuous vetting. VA-CABS demonstrates how VA employs reasonable methods to ensure adherence to the Office of Personnel Management (OPM), and other regulatory issuances in making suitability, fitness, and trust determinations.

(3) Personnel Security Specialists are designated Critical Sensitive/High Risk and require a favorable Tier 5 background investigation. Personnel Security Specialists reviewing and adjudicating background investigations must be trained and certified in OPM Suitability Executive Agent standards. Personnel Security Specialists are authorized to adjudicate employee and affiliate Tier 1, Tier 2, and Tier 4 level investigations as well as Continuous Vetting Alert Reports (CVAR) and RAP Back Alert Reports.

(4) The PSAC is the only authorized entity designated to adjudicate VA Police Officer investigations as well as all Tier 3 and Tier 5 level investigations.

b. **Investigation, Position Designation and Reciprocity Requirements**

(1) VA Administrations, organizations and staff offices will use the OPM and DCSA Position Designation Tool (PDT) for designating position risk (i.e., low, moderate, and high) and sensitivity levels (non-critical sensitive, critical sensitive and special sensitive) for Federal employees, contractor employees and excepted service employees to determine the commensurate level of background investigation.

(2) Personnel Security Specialists play an important role in comparing the nature of the position against the issues in an individual's background when making suitability determinations. Adjudications are case-by-case decisions based upon the nature of the conduct, and the functions and responsibilities of the position.

(3) Per 5 CFR 302.108, VA must make fitness determinations for excepted service positions in accordance with the applicable requirements of 5 CFR Part 731.

(a) Personnel Security Specialists must record its reasons for making fitness determinations under 5 CFR Part 731 and must furnish a copy of those reasons to an applicant upon their request.

(4) Individuals entering employment subject to investigation must undergo a background investigation commensurate with the position designation. Individuals should be initiated before the individual is appointed or otherwise becomes employed by or on behalf of VA, if not prior to appointment, but be done so as soon as possible.

(5) A suitability determination is based on whether an individual's character or conduct may have an adverse impact on the integrity or efficiency of the service. Fitness determinations for contractors or members of the excepted service will be based on the same criteria used to evaluate Federal employees.

(6) Suitability determinations must be made for each appointment in the competitive service or career Senior Executive Service and a fitness determination must be made for each appointment into the excepted service.

(7) Individuals occupying positions of employment subject to investigation are also subject to continuous vetting through periodic checks of their background at any time. Checks must be conducted at regular intervals, based on the type of check and with consideration of position risk and

sensitivity. The nature of a continuous vetting check, and any additional requirements and parameters, will be specified in supplemental issuances.

(8) An individual may be subjected to continuous vetting only if they have signed an authorization for release of information permitting a disclosure for continuous vetting purposes. This release form is contained within Standard Form (SF)-85, SF-85P, and SF-86. Continuous vetting for an individual in a public trust position satisfies the requirement for a periodic reinvestigation of an individual in a public trust position as directed in Executive Order 13488, as amended.

(9) VA must ensure that each continuous vetting check is conducted, and a determination made regarding continued employment.

(10) An individual in a sensitive position who is continually vetted to standards established by the Security Executive Agent for satisfying periodic reinvestigation and/or continuous vetting requirements meets the continuous vetting requirements for a public trust position.

(11) Continuous vetting replaces periodic reinvestigations for individuals occupying public trust and national security positions. Individuals occupying low risk positions are also subject to continuous vetting. These checks are conducted at regular intervals based on the type of check and with consideration of position risk and sensitivity level. Personnel Security Specialists must ensure each continuous vetting check is conducted and a determination made regarding continued employment.

(12) VA must notify each employee of the continuous vetting requirements.

(13) An investigation or continuous vetting check supports a determination of whether the findings of the investigation would justify an action under 5 CFR 731 or another applicable authority such as 5 CFR 315, 359, or 752.

(14) Positions that are intermittent, per diem, or temporary in nature, not to exceed an aggregate of 180 days per year in either a single continuous appointment or series of appointments do not require a background investigation for suitability or fitness. VA, however, does require a favorable Fingerprint Special Agreement Check (FP SAC) for PIV-I eligibility.

(15) All non-U.S. nationals, who have NOT resided in the U.S. or territories for three consecutive years or more, are not eligible for a Tier 1 level investigation. For these individuals, who work for or on behalf of VA, with or without compensation, will be screened using a National Counterintelligence and Security Center sponsored vetting resource. Upon their three-year residency in the U.S. a Tier 1 level investigation must be initiated.

(16) During the investigative process, results may require subsequent review from the VA Insider Threat and Defensive Counterintelligence teams to validate, mitigate, or initiate further actions as appropriate. Personnel Security Specialists will work with the Insider Threat and Defensive Counterintelligence teams prior to making a final determination or to complete adjudication.

(17) VA must reciprocally accept a prior background investigation when the person entering employment subject to investigation has undergone a background investigation that is at or above the level required for the position as determined by the position designation and has a qualifying break in service, unless VA obtains new information in connection with the person's employment that calls into question the person's suitability or fitness.

(18) VA must enroll individuals re-entering service after a break-in-service of 60 months or more, into continuous vetting.

(19) If a prior investigation that is reciprocally accepted, but the Central Verification System or successor system does not reflect a favorable suitability or fitness determination, the Personnel Security Specialist must review the prior investigation to make a new suitability or fitness determination.

c. **Suitability Actions**

(1) VA may take a suitability action in connection with any application for, or appointment to, the competitive service or career Senior Executive Service.

(2) VA's authority to complete a suitability action continues when an application is withdrawn, when an offer of employment is withdrawn, or when an individual appointed separates from employment.

(3) VA's authority to take a suitability action includes the case of an application for or appointment to the competitive service or career Senior Executive Service from another type of position when a prior investigation is being reciprocally accepted.

(4) VA may not take a suitability action against an employee in the competitive service or career Senior Executive Service.

(5) No inquiries into criminal or credit history can occur until a tentative job offer has been made.

(6) The standard for a suitability and fitness determination and for a suitability action is that the action will protect the integrity or promote the efficiency of the service.

(7) If a suitability or fitness issue develops prior to the required investigation, VA may request investigation from DCSA sufficient to resolve the issue and support an unfavorable suitability or fitness determination.

(8) When making a suitability or fitness determination, Personnel Security Specialists must base its suitability determination on the presence or absence of one or more of the specific factors. Only OPM may take a suitability action considering factors listed in paragraph (b)(3) or (7).

3. RESPONSIBILITIES.

a. **Assistant Secretary for Human Resources and Administration/ Operations, Security, and Preparedness** shall:

(1) Advise the Secretary on all matters related to the PVP, and

(2) Provide guidance and oversight to the Chief, Operations, Security, and Preparedness.

b. **Assistant Secretary for Information and Technology and Chief Information Officer** shall: Ensure the Office of Information Security develops and implements a VA Enterprise Information Security Program, commensurate with the Federal Information Security Modernization Act, to protect information resources and to provide security measures commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of VA's information systems.

c. **Inspector General, Veterans Affairs**. The Inspector General Act of 1978 authorizes the Office of the Inspector General (OIG) to select, appoint, and employ officers and employees subject to the provisions of title 5, U.S.C. The Inspector General shall:

(1) Coordinate, initiate, and adjudicate all background investigations for OIG employees in Public Trust and Low-Risk positions.

(2) Determine which OIG positions are national security positions and coordinate with the PSAC for initiation and adjudication.

d. **Principal Executive Director for Office of Acquisition, Logistics, and Construction** shall, in addition to Paragraph e below: Establish regulatory requirements within the Federal Acquisition Regulation and VA Acquisition Regulations (Manuals) for contracts and agreements that require contractors to adhere to personnel vetting procedures in the performance of a contract.

e. **Under Secretaries, Assistant Secretaries, and Other Key Officials** shall:

(1) Comply with policies, actions, processes, and guidelines set forth in this Directive and VA Handbook 0710, Personnel Vetting Program.

(2) Appoint a Personnel Security Program Manager to implement VA's policy and procedures in compliance with the overall Department's PVP.

f. **Chief, Operations Security and Preparedness** shall:

(1) Provide assistance to Under Secretaries, Assistant Secretaries, and Other Key Officials in maintaining effective personnel vetting programs.

(2) Develop, coordinate, and oversee the implementation of policy, programs, and guidance for VA's Personnel Vetting Program, to include setting forth an overarching strategy identifying goals, performance measures, roles and responsibilities associated with the VA PVP.

(3) Ensure that the PVP is consistent, cost-effective, efficient, and balances the rights of individuals with the interests of national security.

(4) Approve, coordinate, and oversee all VA personnel vetting initiatives and activities to improve the efficiency, effectiveness, and fairness of VA's PVP.

(5) Ensure national security clearances are granted only to those persons whose official duties require access to classified information.

(6) Ensure oversight inspections are completed to VA Administrations, and any other approved organizations responsible for personnel vetting.

(7) Represent VA's interests on interagency forums and meetings with national security, suitability, and personnel security concerns, to share best practices, and to actively promote the PVP within the Federal Government.

(8) Serve as VA's Senior Implementation Official regarding Trusted Workforce 2.0.

g. **Executive Director, Personnel Vetting and Credential Management (PVCM)** shall:

(1) Develop, coordinate, and oversee implementation of VA's PVP policy and guidance, including the implementation of the Trusted Workforce 2.0 (TW 2.0) initiative.

(2) Develop Departmental-wide vetting policy to include personnel security, suitability, fitness, and oversight of organizational components' compliance.

(3) Ensure recurring program oversight and reviews of organizations with delegated authority to perform personnel vetting actions.

(4) Ensure the development and implementation of a framework setting forth an overarching strategy identifying goals, oversight and assessment measures, roles and responsibilities, communications strategy, training verification, and metrics to measure the quality of security investigations, suitability and fitness investigations, and corresponding adjudications to ensure a sound PVP that meet the needs of the Department in accordance with Executive Order 13467, as amended.

h. **Chief, Human Resources Officers** shall:

(1) Ensure all appointee and employee positions are designated with the appropriate risk or sensitivity level in accordance with the PDT and ensure each appointee and employee undergo a background investigation commensurate with the position risk or sensitivity level.

(2) Ensure position risk and sensitivity level designations are reviewed by appropriate officials to ensure designations are up-to-date and consistently applied to all positions in accordance with 5 CFR Part 731, Suitability, and 5 CFR Part 1400, National Security Positions.

(3) Ensure appointees and employees have background investigations initiated after a conditional or tentative offer and prior to entrance on duty (EOD) and adjudicated within 90 days of investigation closed date. Adjudicative determinations must be made by appropriately trained personnel.

(4) Ensure an FP SAC is conducted on all new appointees who are exempt from the requirement to have a Tier 1 or higher-level investigation. The FP SAC must be performed prior to the appointee's EOD. Ensure the FP SAC is adjudicated by appropriately trained personnel within five days of receipt.

4. REFERENCES

a. 5 CFR Part 731, Suitability.

b. 5 CFR Part 1400, Designation of National Security Positions.

c. 5 CFR Part 736, Personnel Investigations.

d. EO 12968, Access to Classified Information, as amended.

e. EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified Information.

f. EO 13488, as amended, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust.

g. EO 13764, Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 to Modernize the Executive-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters

h. 32 CFR Part 147, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.

i. 32 CFR Part 2004, Implementing Directive for Executive Order 12958, Classified National Security Information.

j. 32 CFR Part 117, National Industrial Security Program Operating Manual.

k. 18 U.S.C. § 1924, Unauthorized removal and retention of classified documents or material.

l. The Intelligence Reform and Terrorism Prevention Action of 2004 (IRTPA), Public Law 108-458 (December 17, 2004); Title III, Section 3001 (Security Clearances).

m. Federal Information Security Modernization Act of 2014

n. Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors.

o. Federal Information Processing Standards Publication (FIPS) 201, Personal identity Verification (PIV) of Federal Employees and Contractors as amended by FIPS 201-3 or its successors.

p. VA Directive 0735, Personal Identity Verification (PIV) of Federal Employees and Contractors.

q. VA Directive 0327, Insider Threat Policy.

r. VA Directive 6500, Information Security Program

s. VA Handbook 6500, Risk Management Framework for VA Information Systems, VA Information Security Program.

t. Office of Personnel Management (OPM) Memorandum, December 15, 2020, Credentialing Standards Procedures for Issuing Personnel Identity Verification Cards under HSPD-12 and New Requirements for Suspension or Revocation of Eligibility for PIV Credentials (Credentialing Procedures).

u. Federal Personnel Vetting Core Doctrine (FR 2021- 00547) issued in April 2021 by the Director of National Intelligence and the Director, OPM.

v. VA Handbook 5003, Position Classification and Position Management

5. DEFINITIONS.

a. **Affiliate**. A non-Federal employee or contract individual who requires logical access to VA information systems and/or physical access to VA facilities to perform their duties. Examples of affiliates may include (but are not limited to) students, researchers, residents, Veterans Service Organization Officers, volunteers, accredited attorneys, union officials, and interns.

b. **Applicant.** An individual who is being considered or has been considered for employment in the competitive service or career Senior Executive Service. 5 CFR 731

c. **Appointee.** Means an individual who has entered on duty and is in the first year of employment in a competitive service or career Senior Executive Service position when it is employment subject to investigation. When the individual is serving a probationary or trial period, the individual's status as an appointee will extend through the end of the initial probationary/trial period, if longer than one year. 5 CFR 731

d. **Competitive service or career Senior Executive Service**, refers to a position in the competitive service, a position in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and a career appointment to a position in the Senior Executive Service. 5 CFR 731

e. **Confidential.** Is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. Executive Order 13526.

f. **Contractor.** Means an individual who performs work for or on behalf of any agency under a contract and who, to perform the work specified under the contract, will require access to space, information, information technology systems, staff, or other assets of the Federal Government, and who could, by the nature of their access or duties, adversely affect the integrity or efficiency of the Government. Such contracts include but are not limited to personal service contracts; contracts between any non-Federal entity and any agency; and subcontracts between any non-Federal entity and another non-Federal entity to perform work related to the primary contract with the agency. The term contractor employee includes employees of a grantee of any agency or any other category of person who performs work for or on behalf of an agency but does not include a Federal employee. Source: 5 CFR 731

g. **Core Duty.** Means a continuing responsibility that is of particular importance to the relevant covered position or the achievement of an agency's mission. 5 CFR 731

h. **Employee.** Means an individual who has completed the first year of an appointment in the competitive service or career Senior Executive Service when it is employment subject to investigation and is no longer serving the initial probation or trial period, if applicable. In the case of an appointee whose initial probation or trial period is for more than one year, the individual will be considered an employee at the completion of the initial probation or trial period. 5 CFR 731

i. **Employment Subject to Investigation**. Includes an appointment to the competitive service or career Senior Executive Service, an appointment to the excepted service, employment as a contractor employee, or employment as a nonappropriated fund employee. 5 CFR 731

j. **Excepted service** means any position of the executive branch either excepted from the competitive service or which is not in the Senior Executive Service. For the purposes of 5 CFR 731, excepted service does not include:

(1) Any position in an element of the intelligence community as defined in the National Security Act of 1947, as amended, to the extent that the individual is not otherwise subject to OPM appointing authorities;

(2) Any position where OPM is statutorily precluded from prescribing such standards; and

(3) Any position when filled by political appointment.

(4) Senior Executive Service noncareer, limited term, and limited emergency appointments are not subject to suitability actions under this part.

(5) Excepted service does not mean any position excepted from the competitive service of the executive branch that could be noncompetitively converted to the competitive service.

k. **Fitness**. The level of character or conduct determined necessary for an individual to perform work for a Federal agency as an employee in the excepted service, as a contractor employee, or as a nonappropriated fund employee. 5 CFR 731

l. **Fitness Determination**. Means a decision by an agency that an individual has or does not have the required level of character and conduct necessary to perform work for a Federal agency as an excepted service employee. These determinations are based on whether an individual's character or conduct may have an adverse impact on the integrity or efficiency of the service. 5 CFR 731

m. **Material.** In reference to a statement, one that is capable of influencing, affecting, or has a natural tendency to affect, an official decision even if OPM or an agency does not rely upon it. 5 CFR 731

n. **Personal Identity Verification (PIV) Card.** A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains a PIV Card Application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable). VA PIV Cards are issued to persons requiring more than 180 days access to VA facilities or information systems for a period not to exceed 5 years. (Sources: Handbook 0735 and FIPS 201-3, https://csrc.nist.gov/publications/detail/fips/201/3/final)

o. **PIV-Interoperable (PIV-I) Card.** PIV-I credentials do not meet all of the requirements of FIPS 201-3, do not require a background check, a favorable fingerprint check (SAC) is required along with the collection of only two fingerprints, and include an authentication certificate that connects to the Federal Bridge Certificate Authority. Flash PIV-I credentials replaced VA's Non-PIV Cards and Flash Badges.

p. **Reciprocity.** Recognition and acceptance of prior background investigation and favorable adjudications conducted by another Federal agency, without further processing when the determination was based on equivalent criteria.

q. **Risk Designation.** For every position in the competitive service; in the excepted service; to be filled with a career appointment in the Senior Executive Service; or in which the occupant performs a service as a contractor employee or as a nonappropriated fund employee, an agency head must designate the position at high, moderate, or low risk level as determined by the position's potential for adverse impact to the efficiency or integrity of the service.

r. **Secret.** Level of national security clearance, the unauthorized disclosure of which would cause serious damage to the national security'. (Source: Executive Order 12968

s. **Security Clearance.** A determination that a person is eligible for access to classified information.

t. **Sensitivity Designation.** The designation for national security positions, based on the degree of potential damage to the national security, at one of the following three sensitivity levels:

(1) **Special Sensitive position.** A national security position which requires a Tier 5 background investigation and the ability to obtain and maintain a Top-Secret national security clearance with access to Sensitive Compartmented Information.

(2) **Critical Sensitive position.** A national security position which requires a Tier 5 background investigation and the ability to obtain and maintain a Top-Secret national security clearance.

(3) **Non-Critical Sensitive position.** A national security position which requires a Tier 3 or Tier 5 background investigation and the ability to obtain and maintain a Secret or Confidential national security clearance.

u. **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 efficiency of the service.

v. **Suitability Action.** An outcome that may be taken only by OPM or an agency with delegated authority under the procedures in 5 CFR Part 731, subparts C and D.

w. **Suitability Determination.** means a decision by OPM or an agency with delegated authority that an individual is suitable or is not suitable for employment in the competitive service or career Senior Executive Service in the Federal Government or a specific Federal agency. A suitability determination is based on whether an individual's character or conduct may have an adverse impact on the integrity or efficiency of the service.

x. **Suitability Pre-Screening.** Conducting an initial suitability review of an applicant or prospective candidate by a servicing Human Resources office staffing official for entrance into the Federal service or entrance into a higher-level Public Trust or national security position.

y. **Tier 1 Level Investigation.** Investigations conducted to this standard are for positions designated as low risk, Non-Sensitive, and for physical and/or logical access, pursuant to FIPS Publication 201 and HSPD-12, using Standard Form 85, or its successor form.

z. **Tier 2 Level Investigation**. Investigations conducted to this standard are for Non-Sensitive positions designated as moderate risk public trust, using SF 85P, or its successor form.

aa. **Tier 3 Level Investigation**. Investigations conducted to this standard are for positions designated as Non-Critical Sensitive, and/or requiring eligibility for "L" access or access to Confidential or Secret information. This is the lowest level of investigation acceptable for access to classified information using Standard Form 86 or its successor form.

bb. **Tier 4 Level Investigation.** Investigations conducted to this standard are for Non-Sensitive positions designated as high-risk public trust, using Standard Form 85P or its successor form.

cc. **Tier 5 Level Investigation.** Investigations conducted to this standard are for Critical Sensitive/Special Sensitive positions, using SF-86 or its successor form.

dd. **Trusted Workforce (TW) 1.25.** is a transitional state that leverages a risk managed approach to three automated records checks, agency specific information to the extent that it is available within an agency, and event-driven investigative activity to reduce risk. Enrollment in a TW 1.25 capability allows VA to defer periodic reinvestigations for our national security population as week as Public Trust population. VA’s enrollment in DCSA's TW 1.25 capability serves as the foundation upon TW 1.5 and, eventually, TW 2.0 can be built.

ee. **Trusted Workforce 1.50.** TW 1.5 will entail all the high-valued data source records checks to which Tier 3 and Tier 5 enrollees will be subject. At the time DCSA will upgrade their Continuous Evaluation capability to include these data sources, VA's Tier 3 and Tier 5 population will already be enrolled in DCSA's TW 1.25 capability and will be automatically enrolled into the TW 1.5 upgrade. The unenrollment, alert management, and resolution processes will remain the same as TW 1.25. TW 1.5 also includes the adoption of shared services such as National Background Investigation Services and Rap Back.

ff. **Trusted Workforce 2.0.** will transform workforce vetting by employing a modernized and more efficient process for ensuring that only trusted individuals enter and remain in the Federal workforce.

gg. **Top Secret.** Information that which, if disclosed without authorization, could reasonably be expected to cause exceptionally grave damage to national security.