



## MEMORANDUM FOR DISTRIBUTION

SUBJECT: Federal Personnel Vetting Management Standards

### I. Purpose

The Federal Personnel Vetting Management Standards (PVMS) establish requirements for all executive branch departments and agencies (D/As) to execute personnel vetting programs, across all domains (suitability, fitness, national security, and credentialing), using 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. Consistent approaches and practices across the executive branch are essential to achieving the personnel vetting outcomes as specified in the *Federal Personnel Vetting Guidelines*, dated 10 February 2022. D/As will use these PVMS to complement previously issued personnel vetting policies and implementation guidance by the Security Executive Agent and the Suitability and Credentialing Executive Agents<sup>1</sup> (EAs). D/As should use these PVMS to refine internal Trusted Workforce (TW) 2.0 implementation plan.

### II. Authorities

These PVMS are issued by the EAs pursuant to the following authorities:

- A. 50 U.S.C. §§ 3341, 3343, and 3162a.
- B. Public Law 115-232, *National Defense Authorization Act for Fiscal Year 2019*, Section 941, Title 50, U.S.C., Section 3161 (note).
- C. 5 U.S.C. §§ 552a, 1103, 1104, 3301, 3302, and 11001.
- D. Executive Order (E.O.) 12968, Access to Classified Information (2 August 1995), as amended.
- E. E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (30 June 2008), as amended.

---

<sup>1</sup> Per E.O. 13467, as amended, the Director of the Office of Personnel Management is the Suitability and Credentialing Executive Agent, and the Director of National Intelligence is the Security Executive Agent.

SUBJECT: Federal Personnel Vetting Management Standards

- F. E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust (16 January 2009), as amended.
- G. E.O. 13549, Classified National Security Information Program for State, Local, Tribal and Private Sector Entities (18 August 2010).
- H. Presidential Decision Directive/NSC-12, Security Awareness and Reporting of Foreign Contacts (5 September 1993).
- I. Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors (27 August 2004).
- J. 5 C.F.R. Parts 731 and 1400.
- K. Transforming Federal Personnel Vetting, Cabinet Memorandum (14 December 2021).

**III. Scope, Applicability, and Review**

- A. These PVMS are consistent with the *Federal Personnel Vetting Guidelines* that establish the outcomes for successful personnel vetting programs.
- B. These PVMS provide policy requirements for federal personnel vetting programs to effectively and efficiently manage risk across the federal workforce, as provided in the *Federal Personnel Vetting Guidelines*.
- C. These PVMS provide guidance to personnel vetting management practitioners for activities that are performed throughout federal personnel vetting to support greater alignment and integration across complementary mission partners (e.g., Human Resources, counterintelligence, Inspectors General) and, to recruit, manage, and retain a diverse and talented workforce that is trusted to protect people, property, information, and mission.
- D. To the extent permitted by law, these PVMS apply to all persons or entities that participate in federal personnel vetting for or on behalf of the federal government, including:
  - 1. Federal civilian, military, and contractor employee personnel working for or on behalf of the executive branch except as provided by law or E.O.
  - 2. Authorized personnel vetting investigative service providers (ISPs).
  - 3. Authorized adjudicative entities.
  - 4. Trusted Information Providers that corroborate and/or verify data as authorized and commensurate with investigative standards established by the EAs.
  - 5. Executive Branch Shared Service Providers.

**SUBJECT:** Federal Personnel Vetting Management Standards

- 6. Personnel vetting management practitioners such as security, human resources, industrial security, military recruiters, suitability and credentialing practitioners, and others.
  - 7. Personnel vetting oversight entities (e.g., those that conduct program management reviews, assessments, and audits).
  - 8. Any other individual subject to personnel vetting by the executive branch, including state, local, tribal, and private sector personnel.
- E. Internal D/A-level policy must comply with these PVMS absent D/A-specific obligations pursuant to statute or E.O., applicable EA approval, or a waiver or exceptions.
  - F. D/A heads should review their internal policies and procedures periodically to ensure those policies and procedures further the principles, outcomes, and management and policy priorities set forth herein.
  - G. In applying these PVMS, D/As must consult their Senior Agency Official for Privacy (SAOP), or appropriate level designee, to ensure their application protects the privacy and civil liberties of all individuals to ensure consistent treatment, equity, and fairness in accordance with applicable laws and policies.
  - H. The EAs, or their designees, will review these PVMS and subordinate appendices listed below and revise as necessary in response to evolving threats, societal trends, changes to law or policy, research, and innovation, or to accommodate process or technology improvements. At a minimum, the EAs or their designees will review these PVMS every five years.
  - I. These PVMS and subordinate appendices will remain in effect until revoked in writing by the EAs.

<b>Appendix</b>	<b>Title</b>
Appendix A	Personnel Vetting Business Functions
Appendix B	Security Awareness
Appendix C	Reporting Requirements for the Trusted Workforce

**IV. General Policy**

D/As must ensure that all federal personnel vetting activities are conducted in accordance with these PVMS, including the following components of federal personnel vetting programs. Each D/A personnel vetting program must:

- A. Ensure inherently governmental functions are performed by appropriate personnel in accordance with the Office of Management and Budget Circular A-76 and as described in the Federal Acquisition Regulation section 7.503.

SUBJECT: Federal Personnel Vetting Management Standards

- B. Ensure personnel vetting practitioners are trained in accordance with the National Training Standards, as applicable based on duties performed (i.e., background investigator, suitability adjudicator, and/or national security adjudicator).
- C. Ensure personnel vetting practitioners treat all individuals undergoing personnel vetting with fairness, dignity, and respect by adhering to legal and ethical requirements. D/As must ensure personnel vetting practitioners do not engage in unlawful discrimination or take an action that is contrary to applicable policy when conducting personnel vetting activities.
- D. Leverage personnel vetting shared services capabilities as described in the TW 2.0 Shared Services Catalog, where appropriate.
- E. Use the Position Designation System (PDS) for determining associated risk and sensitivity level of positions. The PDS and associated Position Designation Tool provide a method for D/As to designate risk and sensitivity for all positions (e.g., military service members, federal civilian employees, and contractors). D/As should ensure personnel are adequately trained on use of the system and must keep a record of the designation. Refer to 29 July 2022 memorandum *Trusted Workforce 2.0 Implementation Guidance: Updated Position Designation System*.
- F. Ensure personnel vetting practitioners follow guidance for the consistent application of upgrade, transfer of trust, and re-establishment of trust personnel vetting scenarios. Refer to 29 December 2023, and as updated, memorandum *Trusted Workforce 2.0 Implementation and Operational Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Upgrades, Transfer of Trust and Re-establishment of Trust Vetting Scenarios*.
- G. Ensure proper collection, tracking, recording, protection, use, transmission, retention, and sharing of personnel vetting information in accordance with law, regulation, and policy.
- H. Ensure investigative services, including continuous vetting services, are requested only from authorized ISPs.
- I. Adjudicate personnel vetting investigations, including making preliminary determinations, in accordance with the *Common Principles in Applying Federal Personnel Vetting Adjudicative Standards*, dated 19 July 2022.
- J. Use Trusted Information Provider Programs, consistent with policy established in the *Federal Personnel Vetting Investigative Standards and Appendices (Investigative Standards)*, dated 17 May 2022 and as refined, and the *Trusted Workforce 2.0 Implementation and Operational Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Trusted Information Provider Programs Guidance*, dated 1 March 2024, to ensure timeliness, efficiency, and effectiveness by reducing duplicative collection of previously collected information.

SUBJECT: Federal Personnel Vetting Management Standards

- K. Support information-sharing and transparency within and between D/As, industry, and stakeholders for effective personnel, security, and insider risk management in accordance with applicable law, rules, regulations, E.O., and policy.
- L. Enroll individuals into a compliant continuous vetting program and manage enrollments and alerts to identify and monitor insider risk in accordance with the *Investigative Standards*, and implementation guidance.
- M. Maintain an effective reporting program in which the entire workforce understands their roles and responsibilities in identifying and reporting personnel vetting issues to prevent escalation and to protect people, property, information, and mission.
- N. Discontinue in-process investigations including enrollment in continuous vetting when an individual ceases to work, or is no longer seeking work, for or on behalf of the federal government.
- O. Discontinue adjudicative activity when an individual ceases to work or is no longer seeking work, except where ongoing activity or actions is otherwise permissible by policy, regulation, or law.
- P. Establish processes for responding to information requests from other D/As seeking information for the purposes of reciprocally accepting a prior investigation or adjudication, when such requests are consistent with applicable requirements for upgrades, transfer of trust, and re-establishment of trust.

## V. Affiliations

The establishment and management of affiliations with individuals in the applicable government-wide personnel vetting repository(ies) is critical to monitoring human risk. Affiliations designate responsibility for personnel vetting actions and ensure that personnel vetting information is appropriately managed and shared between D/As. These designations promote transparency and support mobility of individuals when they transfer between D/As or maintain affiliations with more than one D/A at a time, known as multiple affiliations. Once EA-designated government-wide personnel vetting repository(ies) capabilities allow for effective and efficient management of affiliations, to include multiple affiliation situations and automation to the greatest extent practicable, D/As must manage affiliations with individuals as follows, notwithstanding any subsequent guidance provided as capability development progresses:

- A. At a minimum, all individuals subject to federal personnel vetting must have a primary affiliated D/A.
- B. Individuals will have only one primary affiliated D/A. All other affiliations will be additional (i.e., second) affiliations.
- C. As described in Section VIII below, D/As with primary affiliation must ensure individuals are enrolled in continuous vetting with an authorized ISP, are responsible for alerting other affiliated D/As if the individual's affiliation with the primary D/A

SUBJECT: Federal Personnel Vetting Management Standards

ends, and must ensure any investigative activity required in response to a continuous vetting alert is conducted by an authorized ISP.

- D. Any D/A processing an individual for vetting who is not currently affiliated with any other D/A must establish and record a primary affiliation with the individual in the applicable government-wide repository(ies). The affiliation must be recorded at the start of the vetting process and communicated to the individual.
- E. Any D/A processing an individual for vetting who is already affiliated with another D/A must establish and record an additional affiliation with the individual in the applicable government-wide repository(ies), except:
  - 1. When the new D/A is vetting the individual at a higher risk and/or sensitivity level than the individual currently is, or has been previously, undergoing vetting, or granting access to national security information at a higher level than previously granted, the new D/A must establish and record itself as the primary affiliation and ensure coordination and notification of the change with the previous D/A that held primary affiliation.
    - a. The D/A establishing a new primary affiliation must resolve any unadjudicated continuous vetting alerts, to include engaging the ISP to perform any required investigative activity, as described in Appendix I, *Investigative Triggers and Required Actions*, of the *Investigative Standards*. The D/A must record the adjudication of the alert in the government-wide repository(ies).
  - 2. When an individual is detailed (or other temporary assignment) to another D/A, the gaining D/A must establish and record an affiliation. The individual's employing D/A will retain primary affiliation. When the detail or temporary assignment ends, the losing agency must end the affiliation.
  - 3. When an individual holds multiple affiliations within a D/A, such as an individual who is affiliated with the Department of Defense as both a military reservist and a civilian, the D/A has discretion to determine which affiliation will be primary to best meet the D/A's risk-management needs.
- F. D/As must discontinue their affiliation in the government-wide repository(ies) when an individual ceases to work, or is no longer seeking to work, for or on behalf of the D/A and/or the federal government.
- G. For the purposes of performance management, the D/A with primary affiliation is responsible for ensuring D/A, ISP, adjudicative entities, and shared service provider collection and reporting of applicable metrics in accordance with the *Performance Management Standards*, dated 14 September 2022, and the *Performance Management Standards Implementation Guidance*, dated 14 November 2023, and as updated.

SUBJECT: Federal Personnel Vetting Management Standards

## VI. Personnel Vetting Scenarios

All federal personnel vetting falls within one of five personnel vetting scenarios in which information about individuals is collected and evaluated to make a trust determination. The five personnel vetting scenarios, as defined by the *Federal Personnel Vetting Guidelines*, are: initial vetting, continuous vetting, upgrades, transfer of trust, and re-establishment of trust.

## VII. Initial Vetting

These PVMS set forth the requirements for managing initial vetting for individuals who have not been previously fully vetted to work for or on behalf of the federal government, or who have been away from government work for a significant period of time (see Re-establishment of Trust). D/As should refer to the *Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agency and Authorized Investigative Service Providers*, dated 31 March 2023, *Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Trusted Information Provider Programs Guidance, Investigative Standards, and Common Principles in Applying Federal Personnel Vetting Adjudicative Standards*.

- A. In accordance with Parts 731 and 1400 of Title 5 of the Code of Federal Regulations (CFR), D/As must ensure each position receives a risk and sensitivity designation according to the PDS issued by the EAs. D/As should refer to *Trusted Workforce 2.0 Implementation Guidance: Update to Position Designation System*.
- B. After the personnel vetting investigation is initiated and the ISP has notified the D/A of the completed required high-yield record checks at the applicable investigative tier, D/As may make a risk-based, preliminary determination of whether to onboard the individual. Preliminary determinations may also include granting temporary eligibility for access to classified information, as addressed in the *Common Principles in Applying Federal Personnel Vetting Adjudicative Standards*, or eligibility for a personal identity credential prior to completion of the investigation and final trust determination. D/As will report preliminary determinations in the applicable government-wide repository and the D/A's internal system of records.
- C. D/A adjudicators will make the final trust determination(s), as required for the position the individual will occupy, in accordance with the *Common Principles in Applying Federal Personnel Vetting Adjudicative Standards* only after the ISP has completed the investigation and provided D/As with the relevant data needed to support a trust determination. D/As must report final trust determinations in the applicable government-wide repository and the D/As' internal systems of records. Upon making and recording a favorable final determination, D/As will enroll the individual into continuous vetting.
- D. If the adjudication process discloses unacceptable risks which warrant an unfavorable trust determination, the D/A will coordinate the appropriate due process, appeal, or redress proceedings commensurate with the domain(s) required of the position. If the

SUBJECT: Federal Personnel Vetting Management Standards

determination remains unfavorable after any applicable due process, appeal, or redress proceedings are completed, the D/A must alert the ISP to disenroll the individual from any subscription-based checks established as part of initial vetting and enter the final determination in the applicable government-wide repository.

### VIII. Continuous Vetting

These PVMS set forth the requirements for managing continuous vetting for individuals who are subject to personnel vetting by the Executive Branch. Investigative requirements for fully developed continuous vetting capabilities are found in Appendix C, *Continuous Vetting Coverage Requirements*, of the *Investigative Standards*. Requirements for transitional states of continuous vetting for individuals in national security sensitive positions are found in the 15 January 2021 memorandum, *Transforming Federal Personnel Vetting: Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0*. Requirements for a transitional state of continuous vetting for individuals in non-sensitive public trust positions, defined as individuals occupying non-sensitive positions designated as moderate or high risk, as defined by 5 CFR 731.106(b), is found in the 8 March 2024 memorandum *Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Continuous Vetting for Non-Sensitive Public Trust Positions*. The EAs may issue additional guidance, as necessary, to adjust transitional state requirements or establish transitional state requirements for additional populations, such as those in non-sensitive low risk positions.

- A. Upon making and recording a favorable determination, D/As will enroll the individual into continuous vetting.
- B. D/As must designate the entities or individuals responsible for collecting and maintaining continuous vetting information (e.g., coordinating between entities, reporting, and maintaining information in the applicable government-wide repository and the D/As' internal systems of records, managing alerts, resolving issues, and handling subsequent personnel vetting actions).
- C. D/As with primary affiliation must ensure individuals are enrolled in a continuous vetting service from an authorized ISP for the duration of their affiliation with the D/A. D/As with additional affiliations must not enroll the individual into a continuous vetting service to avoid duplicative enrollments.
- D. D/As must record continuous vetting enrollments and disenrollments (when affiliation ends) in the applicable government-wide repository(ies).
- E. When an individual with multiple affiliations ends their affiliation with the primary D/A, the primary D/A must notify the D/As with additional affiliations.
  1. The D/A with an additional affiliation that has vetted the individual at the highest risk and/or sensitivity level, or has granted access to national security information at the highest level must establish and record itself as the primary



SUBJECT: Federal Personnel Vetting Management Standards

- affiliation and ensure coordination and notification of the change with all other affiliated D/As.
2. If the individual's vetting level and access level is the same for all D/As with additional affiliations, the D/A that established its additional affiliation at the earliest date must establish and record itself as the primary affiliation and ensure coordination and notification of the change with all other affiliated D/As.
  3. The D/A newly assuming primary affiliation must ensure the individual is enrolled in a continuous vetting service from an authorized ISP for the duration of their affiliation with the D/A.
- F. D/As must evaluate continuous vetting alerts delivered from ISPs or developed from internal sources, such as self-reported information or information from complementary mission areas, and determine whether additional investigative activities are required, as described in Appendix I of the *Investigative Standards*, and evaluate the impact on an individual's trust determination(s) using the *Common Principles in Applying Federal Personnel Vetting Adjudicative Standards* and must report any change in an individual's trust determination(s) in the applicable government-wide repository and the D/As' internal systems of records. Alerts that identify a potential for imminent and serious threat to the individual, others, or a facility must be addressed immediately, as appropriate for the situation.
1. When an individual has multiple affiliations, the D/A with primary affiliation is responsible for coordinating with their ISP to request any required investigative activity as described in Appendix I of the *Investigative Standards*.
  2. When an individual has multiple affiliations, the D/A with primary affiliation must notify other affiliated D/As of the presence of the continuous vetting alert and from the presence of investigative results to ensure all affiliated D/As have an opportunity to make a risk-based decision by evaluating the impact on an individual's trust determination(s).
  3. D/As must report any change in an individual's trust determination(s) (suitability, fitness, national security, and/or credentialing, as applicable) in the applicable government-wide repository(ies).
    - a. In response to new information developed through continuous vetting, only a D/A with primary affiliation may update and report a change in a determination of an individual's eligibility to hold a sensitive position or eligibility for access to classified information.
    - b. D/As with additional affiliations may update and report a change in a determination of an individual's access to classified information at the respective D/A.

SUBJECT: Federal Personnel Vetting Management Standards

4. When a D/A with an additional affiliation develops information from internal agency-specific sources that requires additional investigative activities, as described in Appendix I of the *Investigative Standards*, the D/A must report the continuous vetting alert and coordinate with their ISP to request any required investigative activity. The D/A must notify other affiliated D/As of the presence of the continuous vetting alert and the presence of investigative results to ensure all affiliated D/As have an opportunity to make a risk-based decision by evaluating the impact on an individual's trust determination(s). D/As must report any change in an individual's trust determination(s) in the applicable government-wide repository(ies).

#### IX. Upgrades

An upgrade is usually an internal D/A process for moving individuals into new positions, or assigning them new responsibilities, which require additional personnel vetting because the new position's designation requires an investigation at a higher tier. However, it may also apply as part of the transfer of trust scenario when an individual moves from one D/A to another and requires an investigation at a higher investigative tier. Please refer to the detailed guidance provided in *Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Upgrades, Transfer of Trust, and Re-establishment of Trust Vetting Scenarios*.

#### X. Transfer of Trust

The transfer of trust vetting scenario accounts for the personnel vetting activities required to move a trusted insider from one D/A **to a new** D/A, including but not limited to when:

- A federal employee, or contractor, moves to a new D/A;
- A federal employee, or contractor, moves to a new component within the same D/A;
- A federal employee becomes a contractor, or a contractor becomes a federal employee;
- A contractor moves from one contract company to another (even if sponsored by the same D/A);
- The sponsoring D/A of a contractor's company changes; or
- A contractor's D/A sponsor changes.

Please refer to the detailed guidance provided in *Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Upgrades, Transfer of Trust, and Re-establishment of Trust Vetting Scenarios*.

SUBJECT: Federal Personnel Vetting Management Standards

#### **XI. Re-establishment of Trust**

Federal personnel vetting supports a risk-management approach to re-establishing trust with an individual returning to work for or on behalf of the federal government after a break in service. The re-establishment of trust scenario eliminates redundant personnel vetting actions by focusing on only the key activities required to re-establish a baseline of trust. Please refer to the detailed guidance provided in *Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers – Upgrades, Transfer of Trust, and Re-establishment of Trust Vetting Scenarios*.

#### **XII. Federal Personnel Vetting Record**

These PVMS set forth requirements for managing the Federal Personnel Vetting Record in support of the personnel vetting program across the executive branch. The Federal Personnel Vetting Record is the totality of all personnel vetting-related information maintained on an individual, including vetting actions, investigations, and adjudicative information, and is maintained in the government-wide repositories and/or D/A internal systems of records. Please refer to additional information provided in the *Federal Personnel Vetting Performance Management Standards* and *Federal Personnel Vetting Performance Management Standards Implementation Guidance*.

- A. D/As must establish internal controls to ensure personnel vetting data is adequately safeguarded and access is restricted to persons whose official duties require the information to effectively manage risk to people, property, information, and mission, and for the purposes outlined in the applicable system(s) of records.
- B. D/As should establish internal controls to ensure maintenance of D/A adjudicative personnel records and to keep current individuals' trust determinations for the vetting scenarios mentioned above.
- C. D/As must ensure that any personnel-vetting related information developed about an individual from internal sources, such as self-reported information or information from complementary mission areas, is added to the Federal Personnel Vetting Record, in internal D/A systems of record or the applicable government-wide repository(ies), as pertinent.
- D. D/As should evaluate, where applicable, internal D/A systems of records to ensure readiness for implementation of the *Investigative Standards*. If required, D/A should take action to ready said systems in accordance with the timelines outlined in the TW 2.0 Implementation Strategy.

#### **XIII. Information-Sharing for Personnel Vetting Management**

These PVMS set forth requirements for managing information sharing necessary to support personnel vetting programs across the executive branch. Personnel vetting relies on

SUBJECT: Federal Personnel Vetting Management Standards

lawful and bi-directional sharing of validated relevant information across and within D/As to eliminate unnecessary duplication, reduce waste, improve quality, increase effectiveness, and maximize efficiency, while protecting privacy and civil liberties and ensuring fair and consistent treatment to all individuals. D/A must establish coordination and collaboration in order to establish and maintain effective risk management for their trusted workforce.

- A. D/As will establish an agile information-sharing environment where their complementary mission areas<sup>2</sup> work together to detect risks and support early intervention, fostering an environment where D/As can identify potential risks or vulnerabilities and take preventative measures, to assist individuals and deter potential insider threats to people, property, information, and mission.
- B. D/A personnel vetting programs must manage risk in partnership with complementary mission areas and must establish internal controls necessary to ensure that information sharing within these diverse missions is privacy protective and conducted lawfully for the purpose of addressing risks and identifying potential vulnerabilities so that early intervention and remediation activities can be taken before risks escalate to unacceptable levels.
- C. Information relevant to personnel vetting available from complementary mission areas such as Human Resources, insider threat programs, counterintelligence offices, or Inspectors General programs include, but are not limited to:
  1. Financial issues (tax liens, garnishments, court orders);
  2. Disciplinary actions;
  3. Adverse personnel actions;
  4. Drug-testing results;
  5. Counterintelligence concerns;
  6. Insider threat indicators;
  7. Any other relevant issue information that may impact the individual eligibility.
- D. D/As will ensure information shared among complementary mission areas is recorded in an individual's Federal Personnel Vetting Record, in internal D/A systems of record or the applicable government-wide repository(ies), as pertinent, and acted upon, as appropriate. D/As should assess only credible adverse information or well-founded allegations for potential impacts to an individual's continued eligibility or

---

<sup>2</sup> Complementary mission areas include, but are not limited to: personnel vetting programs, counterintelligence, human resources, employee assistance programs, equal employment opportunity, insider threat, law enforcement (where applicable), information technology, and inspector general.

SUBJECT: Federal Personnel Vetting Management Standards

access. Information shared and recorded is limited to the amount and type of information appropriate for the repository in which it is recorded.

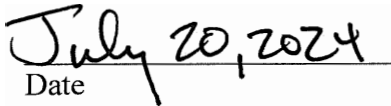
- E. As far as practicable, notifications to personnel vetting management officials should be made as soon as possible to ensure relevant issue information is reviewed and addressed in a timely manner. Additionally, information indicative of immediate threat related to an act of harm, violence, espionage, or destruction of property must be referred promptly to the appropriate insider threat, security, or law enforcement authorities.



Avril D. Haines  
Director of National Intelligence  
Security Executive Agent



Robert H. Shriver, III  
Acting Director  
Office of Personnel Management  
Suitability and Credentialing Executive  
Agent



Date

July 23, 2024  
Date

Attachments:

1. Federal Personnel Vetting Management Standards Appendix A: Personnel Vetting Business Functions
2. Federal Personnel Vetting Management Standards Appendix B: Security Awareness
3. Federal Personnel Vetting Management Standards Appendix C: Reporting Requirements for the Continuous Vetting of the Trusted Workforce

SUBJECT: Federal Personnel Vetting Management Standards

Distribution:

Secretary of State  
Secretary of the Treasury  
Secretary of Defense  
Attorney General  
Secretary of the Interior  
Secretary of Agriculture  
Secretary of Commerce  
Secretary of Labor  
Secretary of Health and Human Services  
Secretary of Housing and Urban Development  
Secretary of Transportation  
Secretary of Energy  
Secretary of Education  
Secretary of Veterans Affairs  
Secretary of Homeland Security  
Administrator, Environmental Protection Agency  
Director, Office of Management and Budget  
United States Trade Representative  
Administrator, Small Business Administration  
Director, Office of Science and Technology Policy  
Director, Office of Administration, Executive Office of the President  
Director, Office of National Drug Control Policy  
Secretary of the Army  
Secretary of the Navy  
Secretary of the Air Force  
Chairman, Joint Chiefs of Staff  
Chairman of the Board of Governors of the Federal Reserve  
Commissioner, Social Security Administration  
Director, Central Intelligence Agency  
Director, National Science Foundation  
Administrator, National Aeronautics and Space Administration  
Administrator, United States Agency for International Development  
Commissioner, Nuclear Regulatory Commission  
Under Secretary for Intelligence and Security, Department of Defense  
Under Secretary for Intelligence and Analysis, Department of Homeland Security  
Director, United States Secret Service  
Director, National Security Agency  
Director, Defense Advanced Research Projects Activity  
Director, Defense Information Systems Agency  
Director, National Reconnaissance Office

SUBJECT: Federal Personnel Vetting Management Standards

Distribution: (continued)

Director, Defense Logistics Agency  
Director, Defense Intelligence Agency  
Director, Defense Contract Audit Agency  
Director, National Geospatial-Intelligence Agency  
Director, Missile Defense Agency  
Director, Defense Finance and Accounting Services  
Commissioner, United States Customs and Border Protection  
Director, Defense Counterintelligence and Security Agency  
Commandant of the Marine Corps  
Chief, National Guard Bureau  
Chairman, Federal Trade Commission  
Chairman, United States International Trade Commission  
Chairman, Federal Communications Commission  
Chairman, Securities and Exchange Commission  
Archivist, National Archives and Records Administration  
Chairman, National Labor Relations Board  
Administrator, General Services Administration  
Director, United States Peace Corps  
Chairman, Federal Maritime Commission  
Administrator, Equal Employment Opportunity Commission  
Director, Bureau of Alcohol, Tobacco, Firearms, and Explosives  
Administrator, Drug Enforcement Administration  
Director, Office of Government Ethics  
Postmaster General, United States Postal Service  
Assistant Secretary for Intelligence and Research, Department of State  
Assistant Secretary for Intelligence and Analysis, Department of Treasury  
Inspector General, Department of Defense  
Director, Selective Service Systems  
Chief Executive Officer, U.S. Agency for Global Media  
Deputy Chief of Staff for Intelligence, United States Army  
Director of Naval Intelligence, United States Navy  
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, United States Air Force  
Director of Intelligence, United States Marine Corps  
Assistant Commandant for Intelligence and Criminal Investigations, United States Coast Guard  
Executive Assistant Director for Intelligence, Federal Bureau of Investigation  
Director, Office of Intelligence and Counterintelligence, Department of Energy  
Chief of Intelligence, Drug Enforcement Administration  
Director, Information Security Oversight Office  
Chief Postal Inspector, United States Postal Inspection Service

## **(U) Federal Personnel Vetting Management Standards - Appendix A: Personnel Vetting Business Functions**

(U) Personnel vetting practitioners play an integral role in assuring the continued trustworthiness of the entire trusted workforce – employees, contractors, military members, and others – who perform work for or on behalf of the Federal Government or other personnel who must undergo personnel vetting. This appendix identifies the core personnel vetting business functions deemed to be inherently governmental as defined by the Office of Management and Budget (OMB) Circular A-76.

(U) Personnel vetting business functions are tasks and activities supporting the personnel vetting process, to include adjudicative activities. These tasks and activities are performed through the five personnel vetting scenarios and apply to each personnel vetting domain: suitability, fitness, national security, and credentialing. The table below describes activities in the personnel vetting business process that are inherently governmental and must be performed by a Federal employee. As a general rule, it is typically the decision-making or approval-granting aspect of a function that is inherently governmental, while non-Federal staff may carry out the activities to execute the decision.

(U) Departments and agencies (D/As) may centralize these personnel vetting business activities within their department or agency or, if otherwise permissible, leverage shared services capabilities or automated business rules along with other decision support tools to improve consistency while performing these functions. For any personnel vetting business activity not listed in the table below, D/As must follow guidance and requirements provided by OMB and in the Federal Acquisition Regulation when determining whether those functions may be performed by non-Federal staff.

(U) This table is UNCLASSIFIED.

<b>Inherently Governmental Personnel Vetting Business Functions</b>	
1.	Approve position designations for risk and sensitivity using the Position Designation System (paper format or automated tool).
2.	Concur with and approve a preliminary determination in any personnel vetting scenario for suitability or fitness; for temporary national security eligibility and/or temporary access; and for interim eligibility to hold a credential (physical or logical access) prior to completion of the investigation.
3.	Approve submission of requests for initial or additional investigation to authorized investigative service provider (ISP) (obligates government funds).
4.	Concur with and sign Statement of Reasons, Letter of Intent, or notices of proposed actions; letters of warning, advisement, or conditions, notices of final decisions/actions or letters of interrogatory.
5.	Concur with and approve any relevant exceptions and/or follow-up requirements required to manage the exceptions; and concur with and approve when an exception may be removed.
6.	Concur with and approve a trust determination in any personnel vetting scenario for suitability, fitness, national security and/or credentialing as applicable to the position.
7.	Make access determination(s)(such as that necessary for Sensitive Compartmented Information or Special Access Program) for an individual who has already been deemed to be eligible for access to classified information (for clarity, the administrative function of recording the determination made is not inherently governmental).
8.	Concur with and approve a decision to suspend or revoke national security eligibility, access to classified information, or credentialing eligibility, to include suspending or revoking temporary or interim eligibility.



<b>Inherently Governmental Personnel Vetting Business Functions</b>	
9.	Concur with and approve a decision to reinstate national security or credentialing eligibility after denial, suspension, or revocation of eligibility.
10.	Concur with and approve a decision to grant one-time (or one-time to a higher level) access to classified information.
11.	Direct and control programs that conduct internal oversight of the D/A's personnel vetting training programs.
12.	Direct and control programs that conduct internal oversight of the D/A's personnel vetting program.
13.	Direct and control programs that conduct quality reviews of the D/A's automated business rules.

## **(U) Federal Personnel Vetting Management Standards Appendix B: Security Awareness**

(U) Departments and Agencies' (D/A) personnel vetting programs must educate the workforce on their responsibilities for identifying potential risks and threats while performing work for or on behalf of the Federal Government. Educating the workforce on their responsibilities and setting clear expectations supports achieving a trusted workforce with a sense of shared responsibility and establishes two-way engagement between the individual and the Federal Government to minimize potential risk to the Federal Government's people, property, information, and mission, a key outcome of the *Federal Personnel Vetting Engagement Guidelines*, dated 10 February 2022. This appendix applies to security awareness briefings used to inform and educate individuals of their responsibilities as a member of the trusted workforce.

### A. (U) Trusted Workforce Briefings

(U) For the purposes of this appendix, the following definitions apply to two types of briefings provided to workforce:

1. (U) **Security Awareness Briefings (SAB)** provide awareness and knowledge of ongoing guidance and procedures to ensure the workforce is aware of security and counterintelligence concerns and responsibilities such as information assurance, both self- and third-party reporting requirements, continuous vetting required actions and compliance, current risk or threat information, cybersecurity, and operational security concerns.
2. (U) **Indoctrinations** convey policy guidance and provide instructions to members of the workforce when granting access to classified national security information (NSI).

(U) The following sections outline the requirements for SABs and indoctrinations, commensurate with the duties and responsibilities of the individual's position.

### B. (U) SAB Requirements for All Individuals

1. (U) Outline the roles and responsibilities of senior security officials, personnel vetting practitioners, and agency-designated personnel who should be contacted in case of questions or concerns about security or personnel vetting matters.
2. (U) Review the types of whistleblower protections afforded individuals based on their position, e.g., military, civilian, employee, or contractor.
3. (U) Additional briefing information may include, but is not limited to:
  - a. (U) Threat awareness and defensive security, including insider threat;

- b. (U) Counterintelligence, including foreign intelligence threats, and espionage (economic and traditional);
  - c. (U) Information security, handling documents, providing security for work papers, and classification procedures;
  - d. (U) Personnel security awareness and duties applicable to the individual's position;
  - e. (U) Continuous vetting requirements;
  - f. (U) Reporting obligations for any behaviors or activities that may affect an individual's status; and,
  - g. (U) Third-party reporting.
4. (U) Before or at the time of issuance of a personal identity verification credential, D/A must provide information in writing to all individuals to ensure individuals are aware of their responsibilities related to the proper handling of such a credential. This information may include, but is not limited to, the following:
- a. (U) Best practices in protecting their identity credential from loss, theft, or damage.
  - b. (U) Best practices for maintaining their credential to prevent unnecessary discovery and association with the D/A, such as removing the credential and storing it in a secure non-visible manner upon leaving the Federal facility or before having their picture taken, not posting copies of the credential on social media, etc.
  - c. (U) Proper procedures on how to report the loss, theft, or destruction of a credential.
  - d. (U) Proper procedures on returning an identity credential upon separation from Federal service.
- C. (U) Indoctrinations for National Security Positions
- 1. (U) Prior to granting individuals access to classified NSI, D/As must ensure compliance with Executive Order (EO) 13526 and 32 Code of Federal Regulation (CFR), Subpart G, *Security Education and Training*.
  - 2. (U) D/As must document that individuals received the indoctrination and SAB in the D/As internal systems of record.

3. (U) D/As must ensure individuals are informed of whistleblower protections specific to their national security position.
4. (U) If an individual has been upgraded to a higher level of access, the D/A must determine whether a new or additional indoctrination or NDA is required. (NOTE: This does not apply to access to Sensitive Compartmented Information (SCI) or Special Access Programs, where a different indoctrination and NDA are required.)
5. (U) Individuals unwilling to comply with the indoctrination, required personnel vetting training as outlined herein, or self-reporting and annual vetting appraisal requirements, should have their access to classified information suspended or denied until compliant, if appropriate, or until determined appropriate by the eligibility/access granting authority(ies).

D. (U) Debriefing

1. (U) D/As must ensure that individuals granted access to classified information receive a debriefing upon leaving employment or when access to NSI is no longer required in accordance with 32 C.F.R. § 2001.
2. (U) D/As may administratively withdraw or revoke access and in those instances, an individual must receive a termination briefing. D/As may administratively debrief an individual in extraordinary circumstances (e.g., the individual is incarcerated, left Government service). Termination briefings must be completed in accordance with 32 C.F.R. § 2001.
3. (U) Upon debriefing from access or completing administrative debriefings, D/As must update the internal D/A records and record the debriefing in the applicable government-wide repository(ies) with the debriefing date.
4. (U) D/As must retain copies of their executed NDAs in accordance with applicable law, regulation, and policy.

E. (U) Personnel Vetting Education and Training Programs

(U) D/As must establish and maintain a personnel vetting education and training program that ensures personnel vetting practitioners are adequately trained to execute their roles and responsibilities in accordance with the laws, rules, regulations, standards, and implementation guidance applicable to Federal personnel vetting, ensuring coverage of the National Training Standards as applicable to the position.

(U) D/As must conduct workforce training to ensure all members of the trusted workforce understand their roles and responsibilities, such as self-reporting, the completion of forms, participation in investigations, protecting identity credentials, and other personnel vetting requirements, as well as D/A-specific security processes, policies, procedures, and organizations.

## **(U) Federal Personnel Vetting Management Standards - Appendix C: Reporting Requirements for the Continuous Vetting of the Trusted Workforce**

(U) Consistent with requirements from the Privacy Act, Federal personnel vetting attempts to gather information directly from individuals, where possible. Individuals are required to self-report information related to their personal history, past behaviors, and conduct during initial vetting when completing investigative forms, and may be required to provide additional follow-up information during the course of the investigation. In continuous vetting, all individuals are subject to Federal personnel vetting throughout their time working for or on behalf of the Government and as such, have a continuing obligation to report when a life event changes information previously reported on their investigative form related to their personal history, activities, conduct and behavior. Collecting this information directly provides the individual an opportunity to disclose the information and provide any relevant context. Disclosure by the individual allows the D/A to potentially provide assistance, where appropriate, while determining the impact of any new information on the individual's eligibility or access, or impact to the integrity and efficiency of the Federal service. Depending on the nature of the life event, the requirement for when to report updated information varies: some information must be updated promptly (further defined below), some in response to ad hoc information requests from the department or agency (D/A), and some on a routine, periodic basis.

(U) This appendix establishes reporting requirements and identifies the specific types of information individuals must promptly report to D/As for processing as part of continuous vetting. For these requirements, to be considered prompt the individual must report the information within three (3) business days of the life event unless prevented from doing so by exceptional circumstances. The reporting requirements for individuals are established commensurate with their position designation.

### **A. (U) D/A Reporting Program Requirements**

(U) Each D/A must establish a program to ensure all individuals subject to Federal personnel vetting who are affiliated with the D/A self-report when life events change information previously reported on the investigative forms in the system(s) designated by the Executive Agents (EAs) for self-reporting. D/As may develop internal systems as needed to collect additional information, where applicable. D/A programs will be established in accordance with supplemental guidance issued by the EAs. D/A programs must:

1. (U) Inform individuals how to report information in the EA-designated system(s) for self-reporting, as well as any applicable internal agency system(s).
2. (U) Provide guidance on any D/A-specific reporting requirements in addition to those provided in Section E, below (e.g., reporting foreign travel plans in advance to allow sufficient time for the D/A to conduct personnel vetting actions or schedule security awareness activities), as well as guidance and procedures for submitting third-party peer and supervisory reporting.

3. (U) Designate roles and responsibilities for D/A personnel vetting managers and practitioners for evaluating the information and conducting or scheduling personnel vetting activities to address reported information.
  4. (U) Integrate reported information with other continuous vetting activities (e.g., continuous vetting alerts, financial disclosure program data, etc.) to compare, contrast and corroborate reported data and identify and manage human risk within the trusted workforce.
  5. (U) Identify, analyze, act upon, and share, as appropriate, relevant reported information with authorized officials in complementary missions, e.g., human resources, security, counterintelligence, Inspectors General, insider threat or law enforcement, etc., to support managing human risk to people, property, information, and mission.
  6. (U) Notify other D/As affiliated with the individual of information that affects any suitability, fitness, credentialing, eligibility status, and access applicable to the individual.
  7. (U) Ensure policy and procedures governing the collection, use, and retention of reported information are in accordance with all applicable legal authorities and include appropriate protections for privacy and civil liberties.
  8. (U) D/As may establish agency-specific reporting requirements to meet statutory obligations or mission need, or to address particular requirements for maintaining eligibility for access to classified national security information or to hold a sensitive position; however, D/As must include the **minimum** reporting requirements for each individual's position risk/sensitivity level.
  9. (U) When an individual is subject to agency-specific reporting requirements, they must report that information directly to the D/A that established those additional requirements. Individuals serving in contractor positions must also notify their private sector security official (e.g., facility security officer) if appropriate.
- B. (U) Notification of Individual Reporting Requirements
1. (U) D/As must notify all individuals subject to vetting who have received a trust determination of their reporting obligations commensurate with their position's risk and sensitivity level. These notifications must:
    - a. (U) provide specific guidance on the sections of the investigative form, or Personnel Vetting Questionnaire (PVQ), and questions that must be promptly updated within three (3) business days upon a change;

- b. (U) designate required timeframes for any D/A-specific reporting requirements in addition to the minimum prompt reporting requirements below, or when advance reporting is required;
  - c. (U) identify the EA-designated system(s) for self-reporting and the processes for submitting information, and the D/A officials to whom information related to any D/A-specific reporting requirements must be reported and what collection methods or mechanisms will be used to collect the required information;
  - d. (U) provide information on how reported information is collected and evaluated and the potential consequences of failure to report as required; and,
  - e. (U) identify D/A assistance available to support individuals in managing personnel vetting risks or vulnerabilities.
2. (U) Notifications should be made at initial on-boarding/indoctrination with refresher training on an annual basis thereafter.

C. (U) Evaluating Reported Information

1. (U) D/As must retain and evaluate reported data with information collected during other continuous vetting activities, such as continuous vetting alerts, self/peer/supervisor/third-party reported information, annual vetting appraisals, security incidents, or other internal agency programs (e.g., insider threat, misconduct investigations, counterintelligence, human resources) to determine if new risk indicators are present or if there are changes in information that was previously reported.
2. (U) D/As must request new investigative activity through their ISP to resolve reported issues that meet the investigative triggers and required actions as specified in Appendix I, *Investigative Triggers and Required Actions*, of the *Federal Personnel Vetting Investigative Standards*.

D. (U) Adjudicating Reported Information

1. (U) D/As or their authorized adjudicative entity must conduct new adjudicative activities to evaluate the reported information and investigative results, if required, to ensure the individual continues to meet eligibility requirements for their position in accordance with the *Common Principles in Applying Federal Personnel Vetting Adjudicative Standards*.
2. (U) The D/A must make a risk management decision whether to add, or modify existing exceptions (e.g., conditions), based on the updated trust determination,

with additional requirements to ensure that issues are addressed/resolved in a timely manner.

3. (U) If the individual's trust determination was previously granted with an exception, D/As must also evaluate whether the new information indicates that the exception has been resolved or should remain in place.
4. (U) If the new information results in an unfavorable trust determination, the D/A must afford the individual the appropriate due process, appeal or review proceedings commensurate with the domain (suitability, fitness, national security, or credentialing) being adjudicated for the position.
5. (U) D/As must also notify complementary mission areas<sup>1</sup>, as applicable, when there are changes in the individual's eligibility status.
6. (U) D/As must ensure reported information is retained in the Federal personnel vetting record including to update the applicable government-wide repository, and, if applicable, the D/A's internal system of records are appropriately and accurately updated.

#### E. (U) Minimum Reporting Requirements

(U) When an individual subject to Federal personnel vetting who has received a trust determination encounters a life event that would change a response previously provided on their investigative form, or Personnel Vetting Questionnaire (PVQ), the individual must report the change in the system(s) designated by the EAs for self-reporting. The sections and questions of the PVQ an individual is required to update promptly when a change occurs is determined by the risk and sensitivity level of the position occupied. The tables below list the minimum reporting requirements for each population based on risk level and national security sensitivity<sup>2</sup>:

- (U) [Low Risk Reporting Requirements](#)
- (U) [Moderate and High Risk Reporting Requirements for Individuals in Non-Sensitive Positions](#)
- (U) [Moderate and High Risk Reporting Requirements for Individuals in Sensitive Positions](#)

(U) The tables identify the sections of the PVQ, and the specific questions within each section, that individuals must update promptly when a life event results in a change to a previously provided response.

---

<sup>1</sup> Complementary mission areas include, but are not limited to: personnel vetting programs, counterintelligence, human resources, employee assistance programs, equal employment opportunity, insider threat, law enforcement (where applicable), information technology, and inspector general.

<sup>2</sup> As additional Trusted Workforce 2.0 policies are finalized, these reporting requirements may be adjusted to align with future issuances.



(U) Because reporting will occur within the PVQ, individuals will be afforded the same protections against self-incrimination for self-reported information as is described in the questionnaire.

(U) Certain information may be required to be reported in advance of the event, such as foreign travel. In such instances, individuals must adhere to D/A-specific guidance and procedures for reporting the information. When advance reporting is required, individuals must still report the relevant information in the PVQ using the EA-designated self-reporting system(s) after the event in accordance with the tables below.

1. (U) Low Risk Reporting Requirements

(U) Table is UNCLASSIFIED

PERSONNEL VETTING REPORTING REQUIREMENTS FOR LOW RISK POSITIONS PVQ SECTIONS REQUIRING PROMPT UPDATES
<p><b>PVQ Section 01 – General Information</b></p> <ul style="list-style-type: none"> <li>• Full name</li> <li>• U.S. Social Security Number</li> <li>• Additional names</li> </ul>
<p><b>PVQ Section 03 – U.S. Citizenship</b></p> <ul style="list-style-type: none"> <li>• Citizenship Status</li> </ul>
<p><b>PVQ Section 04 – Additional Citizenships</b></p> <ul style="list-style-type: none"> <li>• Citizenship of another country</li> </ul>
<p><b>PVQ Section 05 – Residences</b></p> <ul style="list-style-type: none"> <li>• Current residence</li> </ul>
<p><b>PVQ Section 11 – Police Record</b></p> <ul style="list-style-type: none"> <li>• Arrest, charge, conviction, or sentencing for a crime</li> <li>• Domestic violence, restraining, protective, stay-away, no-contact, anti-harassment, or other similar order</li> </ul>
<p><b>PVQ Section 12 – Drug Activity</b></p> <ul style="list-style-type: none"> <li>• Illegal drug use or misuse of a controlled substance (excluding marijuana or cannabis derivatives)</li> <li>• Intentional misuse of prescription drugs</li> <li>• Illegal possession, purchase, manufacture, cultivation, trafficking, production, transferring, shipping, receiving, handling, or sale of any drug or controlled substance (excluding marijuana or cannabis derivatives)</li> <li>• Use of an illegal drug or misuse of a controlled substance while in a national security position (excluding marijuana or cannabis derivatives)</li> <li>• Use of an illegal drug or controlled substance (excluding marijuana or cannabis derivatives) while employed in a criminal justice or public safety position</li> <li>• Ordered to get counseling or treatment as a result of illegal use of drugs or controlled substances (excluding marijuana or cannabis derivatives)</li> <li>• Voluntary counseling or treatment as a result of illegal use of drugs or controlled substances (excluding marijuana or cannabis derivatives)</li> </ul>
<p><b>PVQ Section 13 – Marijuana and Cannabis Derivative Use<sup>3</sup></b></p> <ul style="list-style-type: none"> <li>• Use of marijuana or a cannabis derivative</li> <li>• Use of marijuana or a cannabis derivative while in a national security position</li> <li>• Use of marijuana or a cannabis derivative while employed in a criminal justice or public safety position</li> <li>• Illegal manufacture, cultivation, trafficking, production, transferring, shipping, receiving, handling, or sale of marijuana or a cannabis derivative</li> </ul>

<sup>3</sup> For reporting requirements for all populations, refer to definition of a cannabis derivative as provided in Section 13 of the Personnel Vetting Questionnaire, Office of Management and Budget (OMB) Information Collection 3206-0279, [Personnel Vetting Questionnaire](#).

**PERSONNEL VETTING REPORTING REQUIREMENTS FOR LOW RISK POSITIONS  
PVQ SECTIONS REQUIRING PROMPT UPDATES**

**PVQ Section 17 – Handling Protected Information**

- Illegal or unauthorized access/attempted access of any protected information
- Deliberate non-compliance with rules or regulations for safeguarding protected information

**PVQ Section 18 – Associations**

- Membership in an organization that, at the time of membership, was both (i) dedicated to the use of violence or force to overthrow the United States Government or a State or tribal government of the United States, and (ii) engaged in activities to that end
- Knowing engagement in activities designed to overthrow the United States Government, or a State or tribal government of the United States, by violence or force
- Advocacy for any acts or activities designed to overthrow the United States Government or a State or tribal government of the United States, by violence or force
- Membership in an organization that, at the time of membership, advocated for acts of force or violence to discourage others from exercising their rights under the United States Constitution or the constitution of any State of the United States
- Membership of an organization that at the time of membership, engaged in acts of force or violence to discourage others from exercising their rights under the United States Constitution or the constitution of any State of the United States
- Membership in an organization that, at the time of membership, used unlawful force or violence
- Planning, contributing to, attempting, or carrying out an unlawful act of force or violence targeted at a person, group of people, or property
- Advocacy for unlawful acts of violence against individuals based on their race, color, religion, sex (including pregnancy, sexual orientation, or gender identity), national origin, age, disability, or genetic information
- Membership in an organization dedicated to domestic or international terrorism
- Knowing engagement in any acts of domestic or international terrorism
- Knowing association with anyone involved in activities to further domestic or international terrorism
- Advocacy for any acts of domestic or international terrorism

2. (U) Moderate and High Risk Reporting Requirements for Individuals in Non-Sensitive Positions

(U) Table is UNCLASSIFIED

PERSONNEL VETTING REPORTING REQUIREMENTS MODERATE AND HIGH RISK – NON-SENSITIVE POSITIONS PVQ SECTIONS REQUIRING PROMPT UPDATES
<p><b>PVQ Section 01 – General Information</b></p> <ul style="list-style-type: none"> <li>• Full Name</li> <li>• U.S. Social Security Number</li> <li>• Additional Names</li> </ul>
<p><b>PVQ Section 03 – U.S. Citizenship</b></p> <ul style="list-style-type: none"> <li>• Citizenship Status</li> </ul>
<p><b>PVQ Section 04 – Additional Citizenships</b></p> <ul style="list-style-type: none"> <li>• Citizenship of Another Country</li> <li>• Foreign passport, identity card, or other similar document for international travel</li> </ul>
<p><b>PVQ Section 05 – Residences</b></p> <ul style="list-style-type: none"> <li>• Current Residence</li> </ul>
<p><b>PVQ Section 07 – Employment</b></p> <ul style="list-style-type: none"> <li>• Service in a foreign government</li> </ul>
<p><b>PVQ Section 11 – Police Record</b></p> <ul style="list-style-type: none"> <li>• Arrest, charge, conviction, or sentencing for a crime</li> <li>• Domestic violence, restraining, protective, stay-away, no-contact, anti-harassment, or other similar order</li> </ul>
<p><b>PVQ Section 12 – Drug Activity</b></p> <ul style="list-style-type: none"> <li>• Illegal drug use or misuse of a controlled substance (excluding marijuana or cannabis derivatives)</li> <li>• Intentional misuse of prescription drugs</li> <li>• Illegal possession, purchase, manufacture, cultivation, trafficking, production, transferring, shipping, receiving, handling, or sale of any drug or controlled substance (excluding marijuana or cannabis derivatives)</li> <li>• Use of an illegal drug or misuse of a controlled substance while in a national security position (excluding marijuana or cannabis derivatives)</li> <li>• Use of an illegal drug or controlled substance (excluding marijuana or cannabis derivatives) while employed in a criminal justice or public safety position</li> <li>• Ordered to get counseling or treatment as a result of illegal use of drugs or controlled substances (excluding marijuana or cannabis derivatives)</li> <li>• Voluntary counseling or treatment as a result of illegal use of drugs or controlled substances (excluding marijuana or cannabis derivatives)</li> </ul>
<p><b>PVQ Section 13 – Marijuana and Cannabis Derivative Use</b></p> <ul style="list-style-type: none"> <li>• Use of marijuana or a cannabis derivative</li> <li>• Use of marijuana or a cannabis derivative while in a national security position</li> <li>• Use of marijuana or a cannabis derivative while employed in a criminal justice or public safety position</li> <li>• Illegal manufacture, cultivation, trafficking, production, transferring, shipping, receiving, handling, or sale of marijuana or a cannabis derivative</li> </ul>

<b>PERSONNEL VETTING REPORTING REQUIREMENTS MODERATE AND HIGH RISK – NON-SENSITIVE POSITIONS PVQ SECTIONS REQUIRING PROMPT UPDATES</b>
<p><b>PVQ Section 15 – Federal Debt</b></p> <ul style="list-style-type: none"> <li>• Failure to file a federal tax return or to pay federal taxes</li> <li>• Currently past due on any federal non-tax debt</li> </ul>
<p><b>PVQ Section 17 – Handling Protected Information</b></p> <ul style="list-style-type: none"> <li>• Illegal or unauthorized access/attempted access of any protected information</li> <li>• Deliberate non-compliance with rules or regulations for safeguarding protected information</li> </ul>
<p><b>PVQ Section 19 – Use of Alcohol and Rehabilitative Actions</b></p> <ul style="list-style-type: none"> <li>• Use of alcohol negatively impacts life</li> <li>• Order to get counseling or treatment as a result of alcohol use</li> <li>• Voluntarily went to counseling or treatment as a result of alcohol use</li> </ul>
<p><b>PVQ Section 18 – Associations</b></p> <ul style="list-style-type: none"> <li>• Membership in an organization that, at the time of membership, was both (i) dedicated to the use of violence or force to overthrow the United States Government or a State or tribal government of the United States, and (ii) engaged in activities to that end</li> <li>• Knowing engagement in activities designed to overthrow the United States Government, or a State or tribal government of the United States, by violence or force</li> <li>• Advocacy for any acts or activities designed to overthrow the United States Government or a State or tribal government of the United States, by violence or force</li> <li>• Membership in an organization that, at the time of membership, advocated for acts of force or violence to discourage others from exercising their rights under the United States Constitution or the constitution of any State of the United States</li> <li>• Membership of an organization that at the time of membership, engaged in acts of force or violence to discourage others from exercising their rights under the United States Constitution or the constitution of any State of the United States</li> <li>• Membership in an organization that, at the time of membership, used unlawful force or violence</li> <li>• Planning, contributing to, attempting, or carrying out an unlawful act of force or violence targeted at a person, group of people, or property</li> <li>• Advocacy for unlawful acts of violence against individuals based on their race, color, religion, sex (including pregnancy, sexual orientation, or gender identity), national origin, age, disability, or genetic information</li> <li>• Membership in an organization dedicated to domestic or international terrorism</li> <li>• Knowing engagement in any acts of domestic or international terrorism</li> <li>• Knowing association with anyone involved in activities to further domestic or international terrorism</li> <li>• Advocacy for any acts of domestic or international terrorism</li> </ul>
<p><b>PVQ Section 23 – Financial Record</b></p> <ul style="list-style-type: none"> <li>• Bankruptcy filing</li> <li>• Delinquencies greater than 120 days on alimony or child support payments</li> <li>• Delinquencies greater than 120 days on any debts</li> </ul>
<p><b>Psychological Considerations Information Category Applies Only to Individuals in Certain Select Public Trust Law Enforcement Positions, as Specified by D/A Policy</b></p>

**PERSONNEL VETTING REPORTING REQUIREMENTS  
MODERATE AND HIGH RISK – NON-SENSITIVE POSITIONS  
PVQ SECTIONS REQUIRING PROMPT UPDATES**

**PVQ Section 28 – Psychological and Emotional Health**

- Court or administrative agency order declaring the individual mentally incompetent
- Court or administrative agency order to consult with a mental health professional (An order to a military member by a superior officer is not within the scope of this requirement, and therefore would not require reporting. An order by a military court would be within the scope of the question and would require reporting.)
- Hospital admission, or required hospital evaluation, for any mental health condition or behavioral emergency (Requirement to report includes Include any inpatient hospitalizations, partial hospitalizations, and emergency room visits for a mental health condition(s) or behavioral emergency.)
- Diagnosis by a physician or other health professional with psychotic disorder, schizophrenia, schizoaffective disorder, delusional disorder, bipolar mood disorder, borderline personality disorder, or antisocial personality disorder

3. (U) Moderate and High Risk Reporting Requirements for Individuals in Sensitive Positions

(U) Table is UNCLASSIFIED

PERSONNEL VETTING REPORTING REQUIREMENTS MODERATE AND HIGH RISK – SENSITIVE POSITIONS PVQ SECTIONS REQUIRING PROMPT UPDATES
<p><b>PVQ Section 01 – General Information</b></p> <ul style="list-style-type: none"> <li>• Full Name</li> <li>• U.S. Social Security Number</li> <li>• Additional Names</li> </ul>
<p><b>PVQ Section 03 – U.S. Citizenship</b></p> <ul style="list-style-type: none"> <li>• Citizenship Status</li> </ul>
<p><b>PVQ Section 04 – Additional Citizenships</b></p> <ul style="list-style-type: none"> <li>• Citizenship of Another Country</li> <li>• Foreign passport, identity card, or other similar document for international travel</li> </ul>
<p><b>PVQ Section 05 – Residences</b></p> <ul style="list-style-type: none"> <li>• Current Residence</li> </ul>
<p><b>PVQ Section 07 – Employment</b></p> <ul style="list-style-type: none"> <li>• Service in a foreign government</li> </ul>
<p><b>PVQ Section 11 – Police Record</b></p> <ul style="list-style-type: none"> <li>• Arrest, charge, conviction, or sentencing for a crime</li> <li>• Domestic violence, restraining, protective, stay-away, no-contact, anti-harassment, or other similar order</li> </ul>
<p><b>PVQ Section 12 – Drug Activity</b></p> <ul style="list-style-type: none"> <li>• Illegal drug use or misuse of a controlled substance (excluding marijuana or cannabis derivatives)</li> <li>• Intentional misuse of prescription drugs</li> <li>• Illegal possession, purchase, manufacture, cultivation, trafficking, production, transferring, shipping, receiving, handling, or sale of any drug or controlled substance (excluding marijuana or cannabis derivatives)</li> <li>• Use of an illegal drug or misuse of a controlled substance while in a national security position (excluding marijuana or cannabis derivatives)</li> <li>• Use of an illegal drug or controlled substance (excluding marijuana or cannabis derivatives) while employed in a criminal justice or public safety position</li> <li>• Ordered to get counseling or treatment as a result of illegal use of drugs or controlled substances (excluding marijuana or cannabis derivatives)</li> <li>• Voluntary counseling or treatment as a result of illegal use of drugs or controlled substances (excluding marijuana or cannabis derivatives)</li> </ul>
<p><b>PVQ Section 13 – Marijuana and Cannabis Derivative Use</b></p> <ul style="list-style-type: none"> <li>• Use of marijuana or a cannabis derivative</li> <li>• Use of marijuana or a cannabis derivative while in a national security position</li> <li>• Use of marijuana or a cannabis derivative while employed in a criminal justice or public safety position</li> <li>• Illegal manufacture, cultivation, trafficking, production, transferring, shipping, receiving, handling, or sale of marijuana or a cannabis derivative</li> </ul>

<b>PERSONNEL VETTING REPORTING REQUIREMENTS MODERATE AND HIGH RISK – SENSITIVE POSITIONS PVQ SECTIONS REQUIRING PROMPT UPDATES</b>
<p><b>PVQ Section 15 – Federal Debt</b></p> <ul style="list-style-type: none"> <li>• Failure to file a federal tax return or to pay federal taxes</li> <li>• Currently past due on any federal non-tax debt</li> </ul>
<p><b>PVQ Section 16 – Information Technology Systems</b></p> <ul style="list-style-type: none"> <li>• Illegally or without proper authorization accessed or tried to access any information technology (IT) system</li> <li>• Illegally or without proper authorization tried to and/or did modify, destroy, or manipulate information from an IT system or tried to</li> <li>• Illegally or without proper authorization denied or tried to deny others access to information on an IT system</li> <li>• Illegally or without proper authorization tried to and/or did introduce, use, or remove hardware, software or media from an IT system</li> </ul>
<p><b>PVQ Section 17 – Handling Protected Information</b></p> <ul style="list-style-type: none"> <li>• Illegal or unauthorized access/attempted access of any protected information</li> <li>• Deliberate non-compliance with rules or regulations for safeguarding protected information</li> </ul>
<p><b>PVQ Section 18 – Associations</b></p> <ul style="list-style-type: none"> <li>• Membership in an organization that, at the time of membership, was both (i) dedicated to the use of violence or force to overthrow the United States Government or a State or tribal government of the United States, and (ii) engaged in activities to that end</li> <li>• Knowing engagement in activities designed to overthrow the United States Government, or a State or tribal government of the United States, by violence or force</li> <li>• Advocacy for any acts or activities designed to overthrow the United States Government or a State or tribal government of the United States, by violence or force</li> <li>• Membership in an organization that, at the time of membership, advocated for acts of force or violence to discourage others from exercising their rights under the United States Constitution or the constitution of any State of the United States</li> <li>• Membership of an organization that at the time of membership, engaged in acts of force or violence to discourage others from exercising their rights under the United States Constitution or the constitution of any State of the United States</li> <li>• Membership in an organization that, at the time of membership, used unlawful force or violence</li> <li>• Planning, contributing to, attempting, or carrying out an unlawful act of force or violence targeted at a person, group of people, or property</li> <li>• Advocacy for unlawful acts of violence against individuals based on their race, color, religion, sex (including pregnancy, sexual orientation, or gender identity), national origin, age, disability, or genetic information</li> <li>• Membership in an organization dedicated to domestic or international terrorism</li> <li>• Knowing engagement in any acts of domestic or international terrorism</li> <li>• Knowing association with anyone involved in activities to further domestic or international terrorism</li> <li>• Advocacy for any acts of domestic or international terrorism</li> </ul>
<p><b>PVQ Section 19 – Use of Alcohol and Rehabilitative Actions</b></p> <ul style="list-style-type: none"> <li>• Use of alcohol negatively impacts life</li> <li>• Order to get counseling or treatment as a result of alcohol use</li> <li>• Voluntarily went to counseling or treatment as a result of alcohol use</li> </ul>
<p><b>PVQ Section 20 – Relationship Status</b></p> <ul style="list-style-type: none"> <li>• Current Relationship Status</li> </ul>



<b>PERSONNEL VETTING REPORTING REQUIREMENTS MODERATE AND HIGH RISK – SENSITIVE POSITIONS PVQ SECTIONS REQUIRING PROMPT UPDATES</b>
<p><b>PVQ Section 22 – Foreign Travel</b></p> <p>Individuals must submit an itinerary for unofficial foreign travel according to D/A policy and must receive approval prior to the foreign travel. All deviations from approved itineraries must be reported within five business days of return. When emergency circumstances preclude full compliance with pre-travel reporting requirements, individuals, at a minimum, must verbally advise their supervisor/management chain of the emergency foreign travel with all pertinent specifics requested according to D/A policy, prior to departure, and must fully report the travel within five business days of return. Consistent with national security, D/As may identify conditions under which prior reporting and approval of unofficial foreign travel is not required.</p> <ul style="list-style-type: none"> <li>• Travel to a foreign country</li> </ul>
<p><b>PVQ Section 23 – Financial Record</b></p> <ul style="list-style-type: none"> <li>• Bankruptcy filing</li> <li>• Delinquencies greater than 120 days on alimony or child support payments</li> <li>• Delinquencies greater than 120 days on any debts</li> </ul>
<p><b>PVQ Section 25 – Foreign Contacts</b></p> <p>Contact is not reportable for foreign nationals with whom the contact was only while on official business for the U.S. Government. Contact is defined as communication that is in person; by written correspondence, telephone, electronic media (e.g., email, text, social media, internet, etc.); or other method.</p> <ul style="list-style-type: none"> <li>• Contact with a foreign national</li> <li>• Contact with a foreign national by spouse, legally-recognized partner from a civil union, domestic partnership, common law marriage, or, the person with whom the individual is in a committed, spouse-like relationship</li> </ul>
<p><b>PVQ Section 26 – Foreign Financial Interests</b></p> <ul style="list-style-type: none"> <li>• Ownership of a foreign financial interest by individual; or spouse or legally recognized partner from a civil marriage, civil union, domestic partnership, or common law marriage; or person with whom the individual is in a committed, spouse-like relationship; or a dependent child</li> <li>• Control (not ownership) of a foreign financial interest on someone else’s behalf</li> <li>• Receipt of any educational, medical, retirement, social welfare, or other such benefits from a foreign country by individual; or spouse or legally recognized partner from a civil marriage, civil union, domestic partnership, or common law marriage; or person with whom the individual is in a committed, spouse-like relationship; or a dependent child</li> <li>• Eligibility to receive benefits from a foreign country in the future by individual; or spouse or legally recognized partner from a civil marriage, civil union, domestic partnership, or common law marriage; or person with whom the individual is in a committed, spouse-like relationship; or a dependent child</li> <li>• Provide financial support to a foreign national</li> </ul>
<p><b>PVQ Section 27 – Foreign Business Affairs and Foreign Government Activities</b></p> <ul style="list-style-type: none"> <li>• Advised, supported, or consulted for any foreign-owned business or foreign organization</li> <li>• Request by a foreign government official for advice or to be a consultant made to individual; or spouse or legally recognized partner from a civil marriage, civil union, domestic partnership, or common law marriage; or person with whom the individual is in a committed, spouse-like relationship; or a dependent child</li> <li>• Foreign national offered a job, asked to consider working for them, or asked to be a business consultant</li> <li>• Business venture with a foreign national</li> <li>• Contact with a foreign government agency or its representative by individual or any immediate family members</li> <li>• Sponsorship of a foreign national to the U.S.</li> <li>• Hold political office in a foreign country</li> <li>• Vote in a foreign election</li> </ul>

**PERSONNEL VETTING REPORTING REQUIREMENTS  
MODERATE AND HIGH RISK – SENSITIVE POSITIONS  
PVQ SECTIONS REQUIRING PROMPT UPDATES**

**PVQ Section 28 – Psychological and Emotional Health**

- Court or administrative agency order declaring the individual mentally incompetent
- Court or administrative agency order to consult with a mental health professional (An order to a military member by a superior officer is not within the scope of this requirement, and therefore would not require reporting. An order by a military court would be within the scope of the question and would require reporting.)
- Hospital admission, or required hospital evaluation, for any mental health condition or behavioral emergency (Requirement to report includes Include any inpatient hospitalizations, partial hospitalizations, and emergency room visits for a mental health condition(s) or behavioral emergency.)
- Diagnosis by a physician or other health professional with psychotic disorder, schizophrenia, schizoaffective disorder, delusional disorder, bipolar mood disorder, borderline personality disorder, or antisocial personality disorder

- F. (U) Third-Party Reporting: Peer, Supervisory, and Commander Reporting Requirements
1. (U) To ensure the protection of people, property, information and mission, all individuals in the Executive Branch working for or on behalf of the Government must report to the appropriate D/A official(s) (e.g., designated personnel vetting official(s), Offices of Inspectors General, Insider Threat Programs, Equal Employment Opportunity Offices, etc.) when other individuals demonstrate behaviors or activities that may call into question a trusted insider's conduct, integrity, judgment, loyalty, or reliability.
  2. (U) All members of the trusted workforce, regardless of position designation, must report the following behaviors or activities of other individuals as soon as practical to the appropriate D/A official(s) as soon as it becomes known:
    - a. (U) Unwillingness to comply with rules and regulations or to cooperate with security requirements.
    - b. (U) Unexplained affluence or excessive indebtedness.
    - c. (U) Alcohol abuse.
    - d. (U) Illegal use or misuse of drugs or drug activity.
    - e. (U) Apparent or suspected mental health issues or concerning behavior or conduct where there is reason to believe it may impact the individual's ability to protect classified information or other information specifically prohibited by law from disclosure, or it may endanger the safety or security of others.
    - f. (U) Criminal conduct.
    - g. (U) Misuse of U.S. Government property or information systems.

- h. (U) Loss, compromise, or suspected compromise of classified or controlled unclassified information, or any evidence of tampering with a container used for storage of classified or controlled unclassified information.
- 3. (U) D/As must follow the guidance provided in Section A.7 above regarding the retention, evaluation, and collection of third-party reported information.