PERSONNEL VETTING PROGRAM

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

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This handbook implements the policies contained in VA Directive 0710, Personnel Vetting Program, and revises procedures for managing and administering the VA PVP to include:

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

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

   c. Establishing aligned personnel vetting investigative and adjudicative processes for determining suitability and fitness.

   d. Establishes the requirements when investigations must be conducted for appointments to the civil service or to work as a contractor and/or affiliate.

   e. Removes the periodic reinvestigation requirement for public trust (moderate or high risk) positions.

   f. Establishes the requirements for enrolling populations in low, moderate, or high-risk positions into continuous vetting.

   g. Establishes VA Personnel Security authority for Oversight and Compliance.

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

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 DIRECTIVE:** VA Directive 0710, Personnel Vetting Program, dated September 08, 2025.

5. **RESCISSION:** VA Handbook 0710, Personnel Suitability and Security Program, May 2, 2016.

Department of Veterans Affairs
Washington, DC 20420

VA HANDBOOK 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. SCOPE. 5

3. RESPONSIBILITIES. 5

4. REFERENCES. 7

5. DEFINITIONS. 9

APPENDIX A. PERSONNEL VETTING PROGRAM REQUIREMENTS 12

APPENDIX B. FEDERAL VETTING/SUITABILITY, EXCEPTED SERVICE AND CONTRACTOR EMPLOYEE FITNESS REQUIREMENTS 13

APPENDIX C. NATIONAL SECURITY ADJUDICATIONS AND REQUIREMENTS FOR NATIONAL SECURITY POSITIONS, ELIGIBILITY AND ACCESS TO CLASSIFIED INFORMATION AND/OR SENSITIVE COMPARTMENTED INFORMATION (SCI) .. 25

APPENDIX D. NATIONAL SECURITY DUE PROCESS 30

APPENDIX E. VA CENTRALIZED ADJUDICATION BACKGROUND INVESTIGATION SYSTEM (VA-CABS) 33

PERSONNEL VETTING PROGRAM

1. **PURPOSE.** This handbook establishes and implements policy, procedures, guidelines, program responsibilities, standards and reporting protocols for the VA Personnel Vetting Program (PVP), which includes personnel security, suitability, and fitness determinations for individuals who work for or on behalf of VA. The Federal personnel vetting program 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. The Federal personnel vetting program is aligned with and supportive of the Federal Government's broader efforts to recruit and retain a diverse and talented workforce. The PVP:

   a. Assigns responsibilities and prescribes procedures to conduct background investigations at all tier levels.

   b. Sets procedures for eligibility to occupy a sensitive position and/or national security eligibility for access determinations.

   c. Changes the way in which fitness is determined by aligning the factors and additional considerations used for fitness determinations with those used for suitability.

   d. Prescribes procedures for administrative due process for employees and contractors.

   e. Mandates VA use the same system for designating position risk (i.e., low, moderate, and high) for civil service, contractor employee, and affiliate positions to determine the commensurate level of background investigation. Background investigations conducted for these positions will be done using the same investigative standards, which prescribe the investigative checks to be conducted at low, moderate, and high tiers that correlate to position risk. Finally, agencies will apply the same rules for determining whether reciprocal acceptance of prior background investigation and suitability or fitness determinations are required, promoting efficient transfer of trust determinations.

   f. Establishes the minimum standards of fitness for the excepted service as described in 5 CFR 302.108, which references part 731 for requirements on fitness determinations for excepted positions. Establishes that an agency must record its reason(s) for making fitness determinations under part 731 and must furnish a copy of those reasons to an applicant upon their request. Section 302.203 directs readers to part 731 for the minimum standards and criteria for determining fitness for employment based on character and conduct, allowing agencies to prescribe additional factors to protect the integrity and promote the efficiency of the service when job-related and consistent with business necessity.

2. SCOPE. This handbook applies to all individuals working for, or on behalf of, the VA, with or without compensation, who require access to VA-owned facilities, VA controlled facilities or commercial facilities operating on behalf of VA, VA information technology (IT) systems or their data, or sensitive information and/or access to national security information.

3. RESPONSIBILITIES.

a. **Personnel Security Specialists** shall:

(1) Assist human resources, contracting program and other specialized offices (volunteer, education, etc.) with risk designation for their respective duties to include determination of intermittent positions that do not require an investigation, positions subject only to credentialing standards for badge issuance, and those not eligible for investigations due to United States residency requirements for foreign nationals.

(2) Base suitability determinations on the presence or absence of one or more of the specific factors in 5 CFR 731.202(b) while considering the additional considerations in 5 CFR 731.202(c).

(3) Determine whether the character and conduct of an individual may have an adverse impact on the integrity or the efficiency of the Federal service, by reviewing the report of investigation to identify actionable issues, in accordance with suitability factors, and making an initial assessment of the issues. Information should be analyzed in terms of its relevancy, the nature and seriousness of the conduct, the circumstances surrounding the conduct, the recency of the conduct, the age of the person at the time of the conduct, the contributing societal conditions, the presence, or absence of rehabilitation, as well as the nature of the position for which the person is applying or in which the person is employed.

(4) Meet the requirements of the National Training Standards issued by the Office of Personnel Management (OPM) and the Office of the Director of National Intelligence (ODNI) prior to rendering an adjudicative determination.

(5) Be familiar with laws, regulations, standards, and criteria governing suitability and fitness adjudication.

(6) Be able to obtain and maintain a Tier 5 level investigation.

b. **Human Resources Officers** shall:

(1) Ensure job announcements and notices of personnel action clearly state requirements for suitability and fitness determination and any specific requirement to obtain and maintain eligibility for access to classified information.

(2) Ensure a review takes place whenever an employee is moved from one Position Designation (PD) to another either by promotion, demotion, or re-assignment, to verify the risk and sensitivity level of the position. If the risk or sensitivity level of the position has changed and the incumbent's background investigation is insufficient for the new designation, a new investigation must be initiated within 14 days of the change.

c. **Contract Program or Project Managers** shall:

(1) Ensure appropriate language is included in applicable contracts so that the Statement of Work (SOW) or other defining documentation related to the contract accurately reflects the requirements of this directive and other applicable VA directives and handbooks.

(2) Complete a position designation using the SOW or other defining documentation related to the contract and the OPM, Position Designation Tool (PDT)

d. **Contracting Officers** shall: Ensure appropriate personnel security clauses are included in contracts.

e. **Volunteer Service Officers/Designated Education Officers/Other specialized office leaders** shall:

(1) Document duties and duration of assignment.

(2) Document access required for duties and duration of access to information technology systems.

(3) Document physical access required and duration with special emphasis on access required to restricted areas, drug storage facilities and other areas within facilities that require accountability.

(4) Request risk designation, prescreening, and investigation processing services from local personnel vetting office.

(a) Prescreening and Investigation processing will require PII.

(b) For those personnel that are non-US Persons, additional PII information may be required to complete prescreening or investigation processing.

(5) Ensure all Fingerprint Special Agreement Check (FP SAC), prescreening, and investigation processing is completed according to local personnel vetting office direction.

(6) Ensure local personnel vetting offices are notified of any change in status including, but not limited to, termination, separation, retirement,

resignation, suspension, transfer of position/contract, transfer of duty location, change in affiliation, etc.

4. REFERENCES.

a. VA Directive 0710, Personnel Security and Suitability Program. https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=487&FType=2

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

c. VA Directive 0327, Insider Threat Policy. VA Directive 0327, Insider Threat Policy.

d. Inspector General Act of 1978 igactasof1010.pdf (ignet.gov)

e. VA Handbook 5003/5, Position Classification, Job Grading and Position Management through Change 5. https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=1268&FType=2

f. 5 CFR Parts 302, 315, 332, 338, 359, 731, 732, 736, 752 and 1400 of http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title05/5tab_02.tpl

g. OPM Position Designation Tool (PDT) PDT - Position Designation Tool (nbis.mil)

h. E-Government Act of 2002 E-Government Act of 2002 | National Archives

i. Privacy Act of 1974 Privacy Act of 1974 (justice.gov)

j. Freedom of Information Act, 5 U.S.C. § 552 FOIA

k. 5 U.S.C. § 1104 [USC02] 5 USC § 1104: Delegation of authority for personnel management (house.gov)

l. 5 U.S.C § 3301 [USC02] 5 USC § 3301: Civil service; generally (house.gov)

m. EO 13488, “Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust,” January 17, 2017 https://www.govinfo.gov/content/pkg/WCPD-2009-01-19/pdf/WCPD-2009-01-19-Pg87.pdf, as amended by EO 13764

n. EO 13467, “Reforming Processes Related to Suitability for Government Employment,” https://www.govinfo.gov/content/pkg/WCPD-2008-07-07/pdf/WCPD-2008-07-07-Pg932.pdf

o. EO 13764, “Amending the Civil Service Rules,…,to Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters”,

January 17, 2017, https://www.federalregister.gov/documents/2017/01/23/2017-01623/amending-the-civil-service-rules-executive-order-13488-and-executive-order-13467-to-modernize-the

p. 5 CFR Part 5.4, Information and Testimony. eCFR :: 5 CFR 5.4 -- Information and testimony.

q. EO 12968, "Access to Classified Information" August 4, 1995, as amended https://www.dni.gov/files/NCSC/documents/Regulations/EO_12968.pdf

r. The Intelligence Reform and Terrorism Prevention Act of 2004. E:\PUBLAW\PUBL458.108 (dni.gov)

s. Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances." https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2006/m06-21.pdf

t. Security Executive Agent Directive (SEAD) 4, National Adjudicative Guidelines. SEAD-4-Adjudicative-Guidelines-U.pdf (dni.gov)

u. SEAD 8, Temporary Eligibility. SEAD-8_Temporary_Eligibility_U.pdf (dni.gov)

v. OPM Memorandum, "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)"; December 15, 2020. https://www.opm.gov/suitability/suitability-executive-agent/policy/cred-standards.pdf

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

x. 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. https://csrc.nist.gov/publications/detail/fips/201/3/final

y. National Institute of Standards and Technology (NIST) Special Publication 800-63A, Digital Identity Guidelines, Enrollment and Identity Proofing Requirements. NIST Special Publication 800-63A

z. Presidential Policy Directive (PPD)-19, "Protecting Whistleblowers with Access to Classified Information," issued October 2012 by ODNI. PPD-19.pdf (dni.gov)

5. **DEFINITIONS.**

a. **Adjudication**: The evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is suitable for Government employment.

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 Part 731, https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-731).

c. **Appointee.** 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. (Source: 5 CFR Part 731, https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-731).

d. **Central Verification System**: A data repository for viewing and recording information on existing security clearances, background investigations, suitability, fitness, and HSPD-12 determinations that enables reciprocity among Federal agencies.

e. **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.

f. **Contractor Employee**: 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. https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-731

g. **Continuous Vetting:** Refers to the process of reviewing the background of a covered individual at any time to determine whether that individual continues to meet applicable requirements.

h. **Core duty**: A continuing responsibility of particular importance to the relevant covered position or the achievement of an agency's mission. (Source: 5 CFR Part 731, https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-731).

i. **Covered Position:** Is a person who performs, or who seeks to perform, work for or on behalf of the executive branch or otherwise interacts with the executive branch such that the individual must undergo vetting.

j. **Days**: Calendar days unless otherwise specified in this Handbook. (Source: 5 CFR Part 731, https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-731).

k. **Debarment**: A prohibition from taking a competitive service examination or being hired (or retained) in a covered position for a specific period. Debarment can be issued by an Agency or by OPM. 5 CFR 731

l. **Employee.** 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 Part 731, https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-731).

m. **Material**: In reference to a statement, one that is capable of influencing, affects, or has a natural tendency to affect, an official decision even if OPM or an agency does not rely upon it. (Source: 5 CFR Part 731, https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-731).

n. **Position Designation System and Automated Tool (PDT)**: OPM requires the use of the automated tool in determining the level of risk and sensitivity of positions in the competitive service, positions in the excepted service where the incumbent can be noncompetitively converted to competitive service and initial career appointments in the SES. Position designation determines the type of investigation required for the subject.

o. **Suitability Action:** A suitability action is one or more of the following:

(1) Cancellation of eligibility;

(2) Removal;

(3) Cancellation of reinstatement eligibility; and/or

(4) Debarment.

Source: 5 CFR Part 731, https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-731

p. **Suitability Determination**: 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. (Source: 5 CFR Part 731, https://www.ecfr.gov/current/title-5/chapter-I/subchapter-B/part-731).

q. **Trusted Workforce (TW) 2.0** is a major initiative by the Federal Government to reform personnel vetting. These reforms aim to better support agencies' missions by reducing the time required to bring new hires onboard, enabling mobility of the Federal workforce and improving insight into workforce behaviors.

APPENDIX A. PERSONNEL VETTING PROGRAM REQUIREMENTS

1. **Scope**. These standards cover general PVP requirements.

2. **Personally Identifiable Information (PII).**

   a. Two primary laws, The Privacy Act of 1974 (U.S.C. § 552a) and the E-Government Act of 2002, as amended, set forth requirements for Federal agencies regarding protecting and securing personal information.

   b. These laws regulate the collection, maintenance, use and dissemination of personal information in Government records when that information is retrieved by the subject of record's name or unique identifier.

   c. All VA employees have an obligation to protect information contained in, or extracted from, paper files or automated systems from disclosure.

3. **Personnel Security Record Requirements.**

   a. VA-CABS is the System of Record for background investigation data at the VA.

   b. Original signatures are not required; electronic or facsimile copies are acceptable for personnel security release forms, such as the Standard Form (SF) releases, unless required by Executive Order (EO) or OPM guidance.

4. **Fingerprints.**

   a. FP SAC fingerprints are required for:

      (1) All initial investigations;

      (2) Tier 2 and Tier 4 reinvestigations; and

      (3) Tier 3 and Tier 5 reinvestigations if there are no classifiable fingerprints on file.

   b. Fingerprints are captured and submitted electronically to DCSA using the US Access system.

5. **Freedom of Information Act (FOIA) and/or Privacy Act.** An individual may request copies of their personnel security file under the provisions of the Privacy Act and/or FOIA. The appropriate DCSA FOIA or Privacy Act Office will handle such requests.

APPENDIX B. FEDERAL VETTING/SUITABILITY, EXCEPTED SERVICE AND CONTRACTOR EMPLOYEE FITNESS REQUIREMENTS

1. Scope.

a. This appendix defines suitability and fitness requirements for competitive service Federal applicants, appointees, and excepted service positions where the incumbent can be noncompetitively converted to the competitive service and career appointments into a position in the SES, as defined in 5 CFR Part 731.101(b).

b. This appendix also defines fitness requirements for excepted service Federal applicants and appointees in positions that do not noncompetitively convert to competitive service positions, contractor employees requiring unescorted access to VA-owned facilities, and to affiliates and volunteers and other populations that require access to VA-controlled facilities or commercial facilities operating on behalf of VA, access to VA IT systems and the systems' data; or access to sensitive information.

c. The vetting/suitability process allows for the determination of an individual's suitability for employment based upon an assessment of their character or conduct that may impact the integrity and efficiency of the Federal service.

d. National Security clearances (e.g., Confidential, Secret, and Top Secret) are granted to individuals with a specific requirement for access to classified material and may require an additional investigation and an adjudicative determination.

e. VA, as a member of the National Industrial Security Program (NISP), must conform to all requirements for contractor access to classified material as stated in the National Industrial Security Program Operating Manual (NISPOM). DCSA administers the NISP on behalf of Federal agencies, and VA must use DCSA to process all contractor background investigation requests when national security access is requested and justified. The NISPOM establishes requirements for protecting classified information disclosed to or developed by contractors, licensees, grantees, or certificate holders (hereinafter referred to as contractors) to prevent unauthorized disclosure.

2. Pre-Screening and Interim Suitability Determinations.

a. Initial suitability screenings (pre-screenings) are a required part of the onboarding and background investigative process and can be done at any time after a tentative job offer is extended, contract is awarded, or affiliation with the VA is documented.

b. Upon issuance of tentative offer, contract award, or documented affiliation, the Servicing Personnel Vetting Office (SPVO) shall conduct a pre-screening determination, which involves:

(1) Review of the application and/or resume, and

(2) Review of Optional Form (OF) 306, “Declaration for Federal Employment,”

(3) Review of the results of the electronic fingerprint check, National Criminal History Check, (e.g., FP SAC) and

(4) Review of e-Application within the National Background Investigation Services.

3. Suitability and Fitness.

a. Federal applicants and appointees requiring access to VA facilities and VA IT systems or VA information undergo the requisite background investigation commensurate for their positions’ risk and sensitivity level designation. Title 38 and Title 38 hybrid positions are also subject to investigative and adjudicative guidelines as contained in 5 CFR Part 731.

b. Contractor employees requiring access to VA facilities and VA IT systems receive an appropriate fitness screening/investigation based on the risk level of their positions. The VA program manager and/or business owners are responsible for determining the risk level for each contractor employee position and coordinating with the VA contracting officer to ensure solicitations and contracts include appropriate requirements for contractor employees. The VA program manager will work with Personnel Security Specialists for any assistance needed to use the PDT tool to aid in determining the position designation for contractor positions.

c. Personnel Security Specialists must reciprocally accept a prior background investigation in the event of promotion, demotion, reassignment, or transfer from employment subject to investigation to other employment subject to investigation without a break in service, unless the new employment is at a higher risk level.

d. The appointment of an applicant or appointee to a covered position is subject to a suitability or fitness determination unless exempt per 5 CFR 731.104

e. HRA/OSP VA PERSEC is delegated the authority to conduct departmental oversight and compliance program reviews of VA’s PVP.

f. Adjudications are an inherently Governmental function and must be performed by appropriately trained and favorably adjudicated Federal Government personnel.

g. Personnel Security Specialists shall not discriminate, nor make any negative inferences regarding an individual’s fitness or suitability based on race, color, religion, sex, national origin, disability, or sexual orientation.

h. No person shall be deemed eligible for a national security position as a matter of right or privilege or because of any title, rank, position, or affiliation.

i. Information about individuals collected as part of the investigative and adjudicative process shall be managed in accordance with applicable laws and VA policies, including those related to privacy and confidentiality, security of information, and access to information. Information pertaining to suitability or fitness adjudications will be maintained in accordance with OPM policy.

j. Based on the December 2020 OPM Credentialing Standards Procedure Memo, VA may have specific categories of personnel, such as guest researchers or volunteers who are unique to the agency. However, the credentialing standards procedures set forth in the December 2020 memo generally apply to such personnel unless they are in a short-term position (i.e., less than 6 continuous months). If in a short-term position, the agency has the discretion to vet such personnel for PIV credentials based on risk and other factors or to issue an alternative identity credential with appropriate restrictions and alternative security protections.

4. Position Designation (Risk &Sensitivity) and Investigative Requirements

a. 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

b. Any position subject to risk designation under this section must also receive a sensitivity designation of Special-Sensitive, Critical-Sensitive, Noncritical-Sensitive, or Nonsensitive, as appropriate. This designation is complementary to the risk designation and may have an effect on the position's investigative requirement.

c. If an employee occupies a National Security Sensitive position and/or requires access to classified information to perform assigned duties, the following must be completed before the employee moves to a national security sensitive position.

d. The position designation must be designated at the appropriate national security sensitivity level (Noncritical-Sensitive, Critical-Sensitive, Special-Sensitive). The employee’s Position Description (PD) must be updated to reflect the correct designation.

e. The SHRO must immediately update the HR System of Record to reflect the new position designation.

f. The employee's supervisor must submit VA Form 10097 (Justification for Access to Classified Information or Security Clearance) providing a statement outlining the need for access to classified information. All VHA requests must be routed through the VHA Personnel Security Program Office. Veterans Benefits Administration and National Cemetery Administration 10097 forms must be submitted to Operations and National Security Services (ONSS) for review and approval.

g. Following approval, the employee must complete an SF-86, Questionnaire for National Security Positions, and meet the necessary investigative criteria. This is accomplished by utilizing eApp portal within NBIS.

h. The required investigation must only be initiated by the PSAC.

i. The PD is required to determine the appropriate level of investigation; therefore, all positions within VA are required to have accurate position designations. OPM sets forth guidance on position risk/sensitivity levels and the PDT is provided to simplify and automate the process. VA PERSEC has provided the VA Position Matrix as a general guide for position designation.

j. The PDT will also be used by VA program offices, with support and assistance from VA Personnel Security Specialists, to determine the PD and identify investigative levels for contractors based on the Performance Work Statement or Functional Statement. VA program offices are responsible for determining the risk level for each contractor position and coordinating with the VA contracting officer to ensure solicitations and contracts include appropriate personnel vetting requirements for contractors.

k. All positions must be designated based both on its public trust risk and its national security sensitivity so that the appropriate level of investigation is conducted to address both suitability and national security concerns.

l. Position descriptions and functional statements must be given a risk and sensitivity designation. SHROs, with technical assistance and support provided by assigned Personnel Security Specialists, are responsible for the overall position designation.

m. Position descriptions must be re-evaluated when a position becomes vacant to ensure risk and sensitivity levels have not changed due to new and/or modified duties and responsibilities. This review must also include an updated Position Designation Record generated by the PDT.

n. 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 requires a SAC for these individuals to ensure the suitability or fitness of the person.

o. Intermittent, seasonal, per diem, or temporary positions designated as national security in scope are not exempt from investigation regardless of the length of appointment.

p. VA cannot initiate an investigation if an individual has been in the U.S. for less than 3 continuous years. The OPM Credentialing Standards specify the requirements for vetting Non-U.S. Nationals in support of PIV credential issuance, to include the requirements and processes for employment authorization verification.

(1) VA will utilize a National Counterintelligence and Security Center-sponsored vetting resource for all Non-U.S. Nationals, since a background investigation cannot be completed on a Non-U.S. National who has not lived in the United States for at least 3 continuous years.

(2) PIV credentialing eligibility, which requires a favorable SAC and a minimum of a Tier 1 background investigation, will be determined for all categories of individuals (including HPTs, contractors, and affiliates) based on the above guidance.

5. Investigative Tiers.

a. OPM establishes the level of investigation required for each position risk designation. These standards are used to determine eligibility for logical and physical access, suitability for U.S. Government employment, fitness to perform work for or on behalf of U.S. Government as a contract employee, and eligibility for access to classified information or to hold a sensitive position.

b. The standards consist of five tiers with an Expandable Focused Investigation model at each tier as shown below:

(1) Tier 1 (investigation for positions designated as Low Risk).

(a) This is the minimal level of investigation for a final credentialing determination for logical access.

(b) Tier 1 investigations are requested using the SF-85/SF-85P.

(2) Tier 2 (investigation for non-sensitive positions designated as moderate risk-public trust positions) and are requested using the SF-85/85P.

(3) Tier 3 (investigation for national security positions designated as Noncritical-Sensitive and/or requiring access to Confidential or Secret information) and are requested using the SF-86/86P.

(4) Tier 4 (investigation for High Risk-public trust positions) and are requested using the SF-85/85P.

(5) Tier 5 (investigation for national security positions - Top Secret, sensitive compartmented information, Critical-Sensitive, and Special-Sensitive) and are requested using the SF-86/86P.

c. Public Trust positions are designated as:

(1) Moderate Risk-Tier 2.

(2) High Risk-Tier 4.

d. Personnel Security Specialists must ensure the appropriate level and type of background investigation is requested and adjudicated to determine suitability or fitness for Federal employment of applicant and appointee positions. This action will be accomplished by reviewing the position designation risk level and background investigation information in USA Staffing and VA CABS to include cross referencing on the background investigation case closing transmittal (CCT) summary with all other systems.

e. An investigation should be initiated before the individual is appointed or otherwise becomes employed by or affiliated with VA, or on behalf of VA, however when an investigation is not initiated timely, one must be initiated as soon as possible, even if the appointment or affiliation has already occurred.

f. A change in position risk/sensitivity level requires a background investigation at the new required Tier level. Follow guidance from DCSA regarding OF-306 submission with the background investigation.

g. The individual may remain in the position pending the completion of the new/higher background investigation.

h. Suitability and fitness requirements for employment are separate and distinct from job qualifications (e.g., education or experience requirements). A favorable suitability or fitness determination does not mean that the individual is automatically eligible for a job, and a person who is qualified for a job is not automatically suitable or fit for employment. General suitability or fitness determinations are made after finding the person qualified for the position. Moreover, a final Suitability determination can only be made with a completed, valid background investigation.

i. Record of Arrest and Prosecution Background Investigation (RAP Back) alerts will be reviewed and adjudicated by VA Personnel Security Specialists. and if necessary, referred to the local Employee Labor Relations representative for possible adverse action. For applicants/appointees, RAP BACK alerts will be reviewed by an OPM trained and certified Personnel Security Specialist for possible suitability action. For employees, the alert should be referred to the local Employee Labor Relations staff for possible adverse action.

6. Contractor Fitness Determinations.

a. All contract personnel assigned to work for or on behalf of VA must undergo a background investigation commensurate with the risk and sensitivity level designation associated with the work to be performed at the level indicated in the contract through the PDT. Contractor investigative requirements are based on the length of the contract period of performance, not the number of days the contractor works for VA.

b. The PSAC or Administrations can initiate contractor background investigations, except for national security investigations, as well as adjudicate contractor FP SACs. However, all final adjudicative decisions for contractors must be made by the PSAC. All required investigative documentation must be uploaded and maintained in VA-CABS.

c. Contractor fitness determinations will be performed in the same manner as employee determinations using the suitability criteria of 5 CFR Part 731. VA reserves the right to restrict access to VA facilities, sensitive information, or resources for any contractor, on a need-to-know bases, regardless of the security clearance level.

d. The PSAC will inform contractors who have unfavorable or derogatory information discovered or detected during a personnel investigation and offer the contractor an opportunity to refute, explain, clarify, or mitigate the information in question. The contractor should also be advised that the VA will not disclose any details of the adverse information to the contractor’s employer.

e. If the PSAC makes a final adjudication of unfit on an individual working on a contract, the PSAC will notify the Program Office (or the individual designated by the Program Office) that submitted the request for adjudication of the background investigation for the contractor. The Program Office (or the individual designated by the Program Office), if authorized to communicate with the contractor’s employer under this circumstance, must communicate to the employer (contract company) that:

(1) The contractor is being denied staff-like access for reasonable cause;

(2) Such a finding makes the contractor employee ineligible to render services (or otherwise perform) under the contract; and

(3) The decision by the Government does not intend to imply that the contract employee’s fitness for employment elsewhere in the company is in any way affected by the VA determination on access to VA facilities or information.

7. Suitability/Fitness Reciprocity

a. Investigations and adjudications conducted by other Federal agencies should be reciprocally accepted under Executive Order 13488 whenever possible to

reduce the number of investigation requests, associated costs and unnecessary delays.

b. As with any background investigation request, a check of the Central Verification System (CVS) / Personnel Investigation Processing System must be done to review if a previous investigation has been completed and favorably adjudicated. If the investigation has not been favorably adjudicated within the previous 24 months, the case may be ordered by the Personnel Security Specialist for review and adjudication. If the investigation was not adjudicated and closed more than 24 months ago, a new investigation may be requested.

c. The PSAC must process and approve VA Police Officer and contractor reciprocity.

d. When an individual with a prior, favorably adjudicated investigation moves to a new position either by transfer from another Federal Department or agency or by promotion, demotion or reassignment, a new investigation is not required if the conditions below are met.

(1) The existing investigation is current;

(2) The existing investigation is equal or higher than the investigation required for the new position;

(3) The existing investigation revealed no issues incompatible with the core duties of the new position; and

(4) There was no break in service of 60 months.

e. If an investigation is unavailable, a new appropriate investigation must be initiated.

8. Suitability and Fitness Adjudicative Criteria.

a. Personnel Security Specialists must base suitability and fitness determinations on the presence or absence of one or more of the specific factors listed in 5 CFR 731.202(b).

b. Evaluating whether an individual is suitable or fit to work for the Federal Government (either directly or indirectly as a contractor employee or affiliate) occurs after a background investigation has been completed. Portions of that investigation are conducted by gathering information directly from the individual via personnel vetting forms and, in some cases, personal interviews. Additional information is gathered from other sources.

c. Once the background investigation is complete, the Personnel Security Specialist evaluates the information obtained against the factors. Only conduct falling within a factor may be the basis for finding one unsuitable or unfit. The

Personnel Security Specialist, through application of pertinent additional consideration, will determine whether the individual's character or conduct may have an adverse impact on the integrity or efficiency of the service.

d. Personnel Security Specialists will consider the person holistically, evaluating any impact to the integrity and efficiency of the service on a case-by-case basis.

e. Suitability and fitness determinations are based upon evidence of an individual's character or conduct and when that evidence supports a conclusion that the character or conduct will have an adverse impact on the integrity and efficiency of the service, VA must not make a favorable suitability or fitness determination.

f. Administrations may implement procedures for making Pre-Screening and Preliminary Determinations. The pre-screening determination does not replace the required adjudicative determination for the required background investigation level and does not represent a final suitability determination. Special Sensitive positions do not qualify for pre-screening determinations.

g. Contractor and affiliate fitness requirements are aligned with suitability requirements found in 5 CFR 731.202(b).

h. In making a suitability or fitness determination, the Personnel Security Specialist needs to consider the additional considerations in accordance with 5 CFR Part 731.202.

9. Supplemental Information.

a. If issues emerge during the vetting/fitness process, the scope of the inquiry is expanded as necessary to obtain additional information to assist in the determination of suitability/fitness. If further information from the individual is needed, correspondence may be sent that affords the Federal applicant/appointee or contractor employee the ability to refute, explain, clarify, or mitigate the developed information.

b. The Request for Information (RFI) will include an acknowledged receipt section and requirement for the subject to respond within 10 calendar days of the signature date of the letter. The RFI shall include language that explains the aggravating information, and that should a response not be received, an adjudicative decision will be made with the relevant information available. Extensions may be granted on a case-by-case basis with supervisory approval. However, the 10-day RFI response time will be consistent across the VA.

10. Suitability or Fitness Notifications.

a. When a suitability and/or fitness determination is made (favorable or unfavorable) for competitive, excepted, and Senior Executive service Federal applicants or appointees, the Personnel Security Specialist will notify the subject and respective HR Official/Manager, as appropriate.

b. When a fitness determination is made (fit or unfit), for contractor employees, the VA/Program Office and/or the Contracting Officer (CO) are informed by the PSAC. If a contractor employee is found unfit, a notification is made to the contractor employee that they are ineligible to render services or otherwise perform under the VA contract. Unfavorable information is not disclosed to the contractor employee's company.

c. If the PSAC determines a contractor's conduct (issues in background investigation) is egregious enough and/or a nexus to the position warrants pursuit of temporary and/or permanent removal from all VA contracts, the PSAC will issue the appropriate correspondence to Program Office and/or VA CO.

11. Suitability Action Due Process.

a. When an agency-initiated suitability action is taken against an appointee (within the first year of a subject-to-investigation appointment) the VA SPVO will sign a Notice of Proposed Action (5 CFR Part 731.402).

b. The VA SPVO must notify the appointee (hereinafter, the "respondent") in writing of the proposed action, the charges against the respondent and the availability to request a review of the materials supporting the charges. The notice must outline the specific reasons for the proposed action and state the individual's right to respond to the notice in writing. The notice must provide the VA point of contact (POC) to whom the individual should direct any reply or questions.

c. The notice must also inform the respondent of the time limit for the answer not to exceed 30 calendar days from the signature date of the notice.

d. The notice must explain that the respondent may be represented by a representative of the respondent's choice and that if the respondent wishes to have such a representative, the respondent must designate the representative in writing.

e. The agency must serve the notice of proposed action by mail, secure email, or hand delivery no less than 30 days prior to the proposed action's effective date. The notice must be served to the respondent's last known residence or duty station; and,

f. If the respondent is employed in a position covered by suitability requirements when the notice is served, the respondent may remain in a pay status during the notice period.

g. Should the respondent fail to provide a response within the 30-day period, a final decision will be rendered. Extensions may be granted on a case-by-case bases with SPVO approval.

h. Respondents may submit replies to the Notice of Proposed Action.

(1) The respondent may submit a written response, including affidavits or other written evidence, up to 30 days of the signature date of the notice of proposed action, in accordance with 5 CFR Part 731.403; and,

(2) The respondent may be represented by a representative of choice, at no cost to the Government, if designated in writing.

(3) The Department must issue a decision (in accordance with 5 CFR Part 731.404.

(4) The decision regarding the final action must be in writing, be dated and must inform the respondent of the reasons for the decision and that an unfavorable decision may be appealed in accordance with 5 CFR Part 731; and,

(5) If the decision requires removal, the VA must remove the appointee from the rolls within 5 workdays of the agency's decision.

12. Administrative Procedures.

a. If a VA SPVOs proposes a debarment against an applicant or appointee, the applicant or appointee is entitled to due process and additional procedures apply. The VA SPVO must:

(1) Notify the individual in writing of the proposed debarment as set forth in 5 CFR Part 731.402, including the length of proposed debarment which may be no longer than three years

(2) Explain in the written notice the reasons for the proposed debarment.

(3) Hand deliver, secure email, or mail the written notice to the individual’s duty station or last known residence at least 30 days prior to the effective date of the proposed debarment. The notice must provide the VA POC in VA’s PVP Office to whom the individual should direct any reply or questions.

(4) The individual will be provided an opportunity to explain, mitigate, or refute the reasons for the proposed debarment and submit any evidence in support of the answer as described in 5 CFR Part 731.403. The individual’s written answer must be submitted to the VA POC within 30 days from the notice of proposed debarment.

(5) All debarment proposals, VA and OPM, must be sent to VA’s PVP Office, via the Administration’s Personnel Security Program Office, for review, approval, and/or submission to OPM. If the VA PVP determines that the individual’s character and conduct warrants debarment, the individual will be notified in writing of the final decision to debar the individual from all or specific covered positions within the VA. The notice will include:

(a) The detailed reasons for the debarment;

(b) Information about the individual's right to appeal the final decision to the MSPB; and

(c) A copy of MSPB regulations, 5 CFR Part 1201 and the MSPB Appeal Form 185.

13. Suitability Action Cases Referred to OPM.

a. OPM has the authority to make a final suitability determination and issue suitability actions for employees, issue Governmentwide debarments for applicants, appointees, and employees, where appropriate, and to issue suitability actions in cases where there is evidence of specific types of conduct, which includes cases where there has been:

(1) Material, intentional false statement

(2) Deception or fraud in examination or appointment

(3) Evidence that there has been knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force.

b. When there is evidence of the specific types of conduct, VA SPVOs must refer these cases to OPM. When the VA SPVO determines that a Government-wide debarment or other suitability action by OPM may be an appropriate action, it must refer the case to OPM for consideration.

c. If a Government-wide debarment or other suitability action is warranted, OPM will assume jurisdiction in the case and implement action.

d. If Government-wide debarment or other suitability action is not warranted, OPM will return the case to the VA PVP to complete the suitability determination.

14. Reporting Determinations.

a. All suitability and fitness determinations are recorded in VA-CABS. VA-CABS is the mandatory system used to inform DCSA of adjudicative determinations.

b. Personnel Security Specialists must use VA-CABS to adjudicate cases and cannot report determinations directly to DCSA. Exceptions are approved by VA PVP.

APPENDIX C. REQUIREMENTS TO OCCUPY NATIONAL SECURITY SENSITIVE POSITIONS, ELIGIBILITY AND ACCESS TO CLASSIFIED INFORMATION AND/OR SENSITIVE COMPARTMENTED INFORMATION

1. **Scope.** The principal objective of the national security personnel security adjudicative function is to ensure that individuals who are granted national security eligibility are reliable, loyal, and trustworthy. It involves assessing a sufficient portion of their life history to determine whether they have acted or are acting in ways inconsistent with the adjudicative guidelines. Cases are evaluated using uniform national standards to ensure fair and consistent assessments. Adjudications are performed to determine an individual's eligibility for access to classified information or to hold a sensitive position. National security eligibility determinations are distinct from granting access to classified national security information. This section provides procedures relating to determining national security eligibility.

    a. National security eligibility determinations are made on the merits of the individual case and involve examining a sufficient period of a person's life and background to make an affirmative determination the person is an acceptable national security risk (e.g., where the facts and circumstances indicate granting eligibility is consistent with the national security interests of the United States). Favorable access determinations are made based on the eligible individual's need to access classified information to perform official duties.

    b. All reliable information relevant to determining whether a person meets the national security eligibility standards is reviewed and evaluated only by appropriately trained adjudicative personnel in accordance with appropriate procedures approved by the Security Executive Agent. Final adjudication determinations will be made by PSAC adjudicators.

2. **Prohibition on Retaliation by Affecting Eligibility for Access to Classified Information**.

    a. Security Executive Agent 9 (SEAD 9) establishes policy for employees who seek to appeal an adverse final agency determination with respect to alleged retaliatory action(s) taken by an employing agency affecting the employee's security clearance or access determination as a result of protected disclosures.

    b. SEAD 9 also states each agency is required to have an agency appeal process for whistleblowers that permits employees or former employees alleging reprisals, to appeal the decision affecting their security clearance or access determination within their agency.

    c. Nothing in this handbook limits or affects the independence of the Department of Veterans Affairs Inspector General in fulfilling their duties to determine whether an action affecting eligibility for access to classified information constituted a prohibited reprisal and to recommend appropriate corrective action.

3. Adjudication of National Security Cases.

a. The PSAC is the only entity authorized to initiate and/or adjudicate Tier 3 and Tier 5 cases.

b. If an individual is determined suitable for employment and the position is designated as a national security sensitive position, the national security guidelines are applied to determine whether the individual meets the standards to encumber a national security position or for eligibility to access classified information.

c. Those occupying a national security position must complete the SF-86 “Questionnaire for National Security Positions.” National security investigations are conducted in accordance with Federal Investigative Standards.

d. Access to classified information is limited to employees whose official duties require knowledge or possession of the information. No one has a right to access classified information solely by office, rank, or position.

e. Classified Information Non-Disclosure Agreement (SF-312).

(1) As a condition of being granted access to classified information, the individual must first undergo a security briefing. The briefing is administered by the Office of National Security Services (ONSS). The individual is informed of the obligations and responsibilities contingent upon being granted such access and must execute the SF-312.

(2) The signed, and witnessed, SF-312 will be uploaded into VA-CABS (VA Centralized Adjudication Background Investigation System).

4. National Security Sensitive Levels and Investigative Requirements.

a. The position sensitivity level is based on an overall assessment of impact that an individual could cause to national security.

b. Position designation is required to determine the appropriate level of National Security investigation; therefore, all positions within VA are to be designated. OPM and ODNI set guidance on position risk/sensitivity levels and the PDT is provided to simplify and automate the process.

c. Individuals occupying national security sensitive positions must be enrolled into Continuous Vetting (CV). CV enrollment is coordinated by the PSAC with the Defense Counterintelligence and Security Agency (DCSA).

d. CV has replaced the requirement for periodic reinvestigations.

e. Any position receiving a position sensitivity designation at the CS or SS level shall automatically carry a High Risk designation in accordance with 5 CFR Part 731.106, without requiring further action from the Department.

f. Any position receiving a sensitivity designation at the NCS level shall receive a Moderate Risk designation, in accordance with 5 CFR Part 731.106, unless the agency determines that the position should be designated at the high level. In those instances, supervisors shall designate the position at the high level where warranted based on criteria set forth in OPM issuances as described in 5 CFR Part 731.102(c).

g. For National Security Sensitive positions, background investigations should be scheduled prior to entrance on duty day. Waivers to this requirement may be requested through the VA PVP office, provided the waiver meets the requirements in SEAD-8, Temporary Eligibility.

h. For all National Security Sensitive positions, investigations can be completed post-appointment contingent upon:

(1) Favorable review of the SF-86,

(2) Favorable review of pre-employment checks as outlined in SEAD-8, and

(3) Expedited submission of the request for investigation.

5. Reciprocity of Background Investigations and National Security Adjudications.

a. Security Executive Agent Directive 7, Reciprocity of Background Investigations and National Security Adjudications, establishes requirements for reciprocal acceptance of background investigations and national security adjudications for initial or continued eligibility for access to classified information or eligibility to occupy a sensitive position.

b. VA reciprocally accepts existing national security eligibility determinations or clearances from other Federal Government agencies in accordance with SEAD-7.

6. National Security Adjudicative Guidelines.

a. National security sensitive positions are adjudicated using the national security adjudicative guidelines according to SEAD-4, National Security Adjudicative Guidelines.

b. Eligibility shall be determined by appropriately trained adjudicative personnel through the evaluation of all information bearing on an individual's loyalty and allegiance to the United States, including any information relevant to strength of character, honesty, discretion, sound judgment, reliability, ability to protect classified or sensitive information, and trustworthiness.

c. Eligibility for access to classified information or eligibility to occupy a sensitive position shall only be granted when the evaluation of all such information demonstrates that such eligibility is clearly consistent with the interests of the United States: any doubt shall be resolved in favor of the national security.

d. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. The adjudication process carefully weighs several variables known as the whole-person concept. Available, reliable information about the person, past and present, favorable, and unfavorable, should be considered in reaching a determination.

e. The ultimate determination of whether the granting or continuing of national security eligibility is clearly consistent with the interest of national security must be an overall common-sense judgement based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person.

f. Each case is judged on its own merits and final determination remains the responsibility of the PSAC. Any doubt concerning personnel being considered for access to classified information is resolved in favor of national security. No person shall be deemed to be eligible for a national security position merely by reason of Federal service, licensee, certificate holder or grantee status, as a matter of right or privilege, because of any title, rank, position or affiliation. No person shall be appointed or assigned to a national security position when an unfavorable personnel security determination has been rendered.

g. The ability to develop specific thresholds for action under these guidelines is limited by the nature and complexity of human behavior. The ultimate determination of whether to grant or continue eligibility for a security clearance is clearly consistent with the interests of national security and is an overall common-sense judgment based upon careful consideration of the guidelines outlined in EO 12968.

h. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole-person concept, the pursuit of further investigation may be terminated by the PSAC in the face of reliable, significant, disqualifying, or adverse information.

i. If, after evaluating information of security concern, the Personnel Security Specialist decides that the information does not warrant a recommendation of denial or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access as outlined in SEAD 4.

7. Interim Access.

a. SEAD 8, Temporary Eligibility, applies to any executive branch agency, authorized investigative agency, or any authorized adjudicative agency conducting background investigations and adjudications for temporary eligibility.

b. The PSAC is the only authorized entity to approve temporary access to classified information, temporary access to a higher level of classified information, one-time access to classified information, temporary eligibility to hold a sensitive position, and temporary eligibility to hold a higher-level sensitive position. Temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, during exceptional circumstances where official functions must be performed prior to completion of the investigation and adjudication process.

c. The temporary eligibility will be valid until the exceptional circumstances have abated, the temporary access is terminated, or completion of the investigation and adjudication; however, the VA may revoke it at any time based on unfavorable information identified during the investigation.

d. These temporary eligibilities, also known as “Interim” eligibilities, are completed during exceptional circumstances when official functions must be performed, to include meeting mission readiness requirements, pursuant to EO 12968, as amended. The interim eligibility is made concurrently with the initiation of the investigation and will generally remain in effect until an investigation is completed, at which time the applicant is considered for a final eligibility.

e. Requests for employees and contractors who have been granted interim/temporary eligibility for access to classified information and/or temporary eligibility to occupy a sensitive position, by another Federal agency will be reviewed on a case-by-case basis.

f. If the other Federal agency granted the interim eligibility and it is verified by the CVS or by official letterhead memorandum, the PSAC will review and apply reciprocity to the interim determination. The originating Federal agency is responsible for the final adjudication of the investigation. When the final determination has been made, the requesting office will be responsible for providing an update to the PSAC.

APPENDIX D. NATIONAL SECURITY DUE PROCESS

1. **Scope.** Applicants and employees who are determined to not meet the standards for access to classified information must provide as comprehensive and detailed a written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permits.

   a. **A Letter of Intent (LOI).** The LOI to deny or revoke must accompany or include the Statement of Reasons (SOR) and contain:

      (1) A summary of the security concerns and supporting adverse information.

      (2) Instructions for responding to the SOR.

   b. **A Written SOR.** The SOR must provide a comprehensive and detailed written explanation of the basis for that conclusion as the national security interests of the United States and other applicable law permits. The SOR must explain each security concern, state the specific facts that trigger each security concern, identify the applicable adjudicative guideline(s) for each concern, and provide the disqualifying conditions and mitigating conditions for each adjudicative guideline cited. The statement must also include instructions for responding to the concerns.

   c. **An Opportunity to Reply to the LOI and SOR.** The reply must be in writing to the PSAC.

      (1) The individual must notify the PSAC in writing within 10 calendar days of receipt of the LOI and SOR whether they intend to reply to the LOI and SOR.

      (2) The individual's reply to the LOI and SOR must be submitted no later than 30 calendar days from the date they received the LOI and SOR. An extension of up to 30 calendar days from the original deadline may be granted by the employing organization following submission of a written request from the individual. Requests for extensions must be submitted before expiration of the original deadline. Additional extensions may only be granted by the PSAC when factors beyond the individual's control (e.g., failure of the DCSA to provide records in a timely manner) warrant granting additional time.

      (3) The PSAC will not deny or revoke an individual's national security eligibility without official documentation that the individual received the LOI and SOR.

   d. **Written Letter of Denial (LOD) or Letter of Revocation (LOR).**

      (1) When a favorable determination cannot be rendered, the PSAC will provide the individual a letter documenting the reason(s) for denying or revoking

national security eligibility, as the national security interests of the United States and other applicable law permits.

(2) The LOD or LOR will include clear instructions on how to appeal the unfavorable determination, of the right to be represented, of the right to request documents upon which denial or revocation is based, and of the right to request the entire investigative file, as permitted by national security and other applicable law.

(3) The PSAC will provide the written LOD or LOR as promptly as individual circumstances permit but no more than 60 calendar days from the date of receipt of the individual's reply to the SOR and LOI, provided no additional information is deemed necessary to render the national security eligibility determination.

(4) When a LOD or LOR is based on an individual's failure to reply to the SOR and LOI, the LOD or LOR will include all of the security concerns, adjudicative guidelines, mitigating factors contained in the SOR and LOI, and the reason(s) for denying or revoking national security eligibility.

(5) The individual will be notified in writing if a LOD or LOR cannot be completed within the time frame allowed. The notification shall include the reasons why, and the date the written LOD or LOR is expected to be completed, which will not normally exceed a total of 90 calendar days from the date of receipt of the reply to the SOR and LOI.

(6) The PSAC will notify the individual within 10 calendar days if they are unable to deliver the LOD or LOR. The notification will include information explaining why the LOD or LOR could not be delivered (e.g., illness or death in the family, deployment) and when the individual can expect to receive a copy of the LOD or LOR. The PSAC must deliver the LOD or LOR immediately upon the individual's return.

e. **An Opportunity to Appeal the LOD or LOR.**

(1) Within 10 calendar days of receipt of LOD or LOR, the individual must sign and return the notice of intent to appeal (NOIA) to the PSAC. The individual must state whether they intend to appeal and if so, whether they request a personal appearance or will appeal in writing. The PSAC may grant a single 10 calendar-day extension upon request from the individual.

(2) The PSAC will store signed statements acknowledging receipt of LOD or LOR and NOIA electronically in the subject's adjudicative record.

(3) If the individual elects to appeal the LOD or LOR, the PSAC will forward a copy of the NOIA within 2 calendar days to the ONSS who will coordinate with the Security Appeals Board (SAB). The SAB is comprised of three individuals who are appointed by the VA Secretary, or designee, The

PSAC will also forward the individual's adjudicative record within two calendar days to ONSS. The adjudicative record will contain all the materials the PSAC relied upon to render its determination and the LOI, SOR, LOD, or LOR, and any rebuttal materials the individual provided in response to the LOI/SOR.

f. **Appealing the LOD or LOR to the SAB.** If a decision is made to appeal the LOD or LOR, individuals may do so by:

(1) Sending a written appeal directly to, or personally appear before, the SAB. Individuals must, within 30 calendar days of receipt of a LOD or LOR, write to the SAB stating reasons why the denial or revocation should be overturned and provide any additional relevant information that may have a bearing on the case.

(2) The appeal and supporting documentation will be transmitted to the PSAB via ONSS. The PSAB chair may grant a 30-calendar day extension of time for good cause demonstrated by the appellants (e.g., illness or death in the family, deployment).

g. **A Final Written Decision by the SAB.** The SAB will review the adjudicative file and any appeal materials to render a final decision. If the SAB agrees with the PSAC's written recommendation, the SAB may adopt the written recommendation in lieu of providing a SAB written determination. The individual will be notified of the SAB's final determination via the individual's Human Resources Office, generally within 45 calendar days of the receipt of a direct appeal or 30 calendar days from receipt of the recommendation. The VA SAB's written decision will identify each adjudicative guideline issue stated in the LOD or LOR that formed the basis of the denial or revocation that remains unmitigated after the appeal and the rationale for the final disposition of the appeal.

APPENDIX E. VA CENTRALIZED ADJUDICATION BACKGROUND INVESTIGATION SYSTEM (VA-CABS)

1. **Scope.** This Appendix describes VA-CABS, a web-based personnel security case management tool designed to support the lifecycle of VA personnel security, suitability, fitness, and credentialing cases, including the capture of information related to background checks, investigations, and final determinations. The roles and responsibilities described in this appendix are related only to the use and functions within VA-CABS.

2. **VA-CABS System Description.**

   a. VA-CABS provides a common repository for personnel security records across VA. VA-CABS can shift personnel security resources from one VA SPVO to another for surge support without incurring extensive re-training.

   b. VA-CABS supports the lifecycle of VA's personnel security, administrative security, and management records to include capturing the data related to suitability determinations, background investigations, and security clearance processing. The records in this system reflect the tracking/status of activities related to the management and implementation of personnel security, suitability, and fitness programs that support the protection of the Department's personnel, property, facilities, and information.

3. **Roles and Responsibilities.**

   a. **VA Subject** is any VA employee, contractor, trainee, volunteer, or affiliate who is the subject of an FP SAC or a background investigation. VA subjects:

      (1) Complete fingerprinting;

      (2) Complete electronic questionnaire via DCSA automated system and any other required supporting documents;

      (3) Provide updates on incomplete information and, if necessary, provides additional details; and

      (4) Respond to adjudicative actions and requests.

   b. **Security Assistant** is a VA employee responsible for assisting in the execution of personnel security related functions. Within a determined jurisdiction, the Security Assistant:

      (5) Receives OF-306s, resumes, and any other supporting documents for attachment to a VA Subject profile.

      (6) Completes prescreening determinations and documentation within VA-CABS cases linked to new positions.

c. **Security Specialist** is a VA employee responsible for the execution of personnel security related functions. Personnel Security Specialists' access is normally limited to their assigned organization:

(1) Conducts a quality review of the SF-85/85P or SF-86/86P and approves it for release to DCSA;

(2) Determines that the FP SAC is complete, makes the adjudicative determination, documents adjudicative actions in VA CABS, and reports the adjudicative determination to the subject;

(3) Performs adjudications for background investigation in a timely and efficient manner and is accountable for his/her performance;

(4) Reviews cases for reciprocity and debarment; and

(5) Adheres to all Personnel Security Program Standard Operating Procedures, Policy, Advisories, Regulatory Guidance, and applicable laws.

(6) Runs reports on cases within the SPVO for compliance and governance reporting;

(7) Performs second-level review of cases for quality assurance;

(8) Conducts audits of adjudicative actions and is accountable for adjudicative determinations under their purview; and

(9) Ensures the adjudicative team follows Standard Operating Procedures, Policies, Advisories, Regulatory guidance, and applicable laws.

d. **Case Manager** is a VA employee at an organization level (e.g., Veterans Integrated Service Network (VISN) or Regional Office (RO)) responsible for overseeing the administration of cases across SONs and SOIs within that organization. Within their assigned organization, the Case Manager:

(1) Has all accesses equivalent to the Personnel Security Specialist within the SPVO;

(2) Reviews cases for quality assurance (in-process and adjudicated cases);

(3) Is authorized to reassign cases within their organization for adjudication;

(4) Runs reports on cases within the VISN or RO compliance and governance reporting.

(5) Acts as the point of contact for all insider threat cases. Case manager can view but not edit insider threat cases for assistance in mitigation of insider threat issues.

e. **Read-Only Reviewer** is a VA employee or contractor with read-only privileges for VA Subject profiles within VA-CABS. The Read-Only Reviewer:

(1) Views details of closed cases on a need-to-know basis;

(2) Is authorized to review case documents for adjudicated cases on a need-to-know basis; and

(3) Is authorized to run reports on cases on a need-to-know basis.

f. **Insider Threat Reviewer** is a VA employee that can review and edit certain records of VA Subjects in VA-CABS based on Insider Threat concerns. Authorized to view cases in VA-CABS. The Insider Threat Reviewer is:

(1) Authorized to upload attachments (e.g., SF-312) to cases of VA Subjects;

(2) Authorized to make free text annotations on cases that: (a) the System Owner has granted the reviewer permission for; or (b) Personnel Security Specialists have marked for insider threat indicators;

(3) Authorized to place a profile on hold pending completion of required Insider Threat or defensive counterintelligence action items; and

(4) Authorized to request access to specific cases to make post adjudication modifications.

g. **System Owner** is a VA employee that has elevated privileges to make changes within VA-CABS. The System Owner is:

(1) Authorized to pull and create reports on a SON, VISN and enterprise level;

(2) Authorized to review case documents for adjudicated cases;

(3) Authorized to reassign cases within the SON and between SONs for adjudication; and

(4) Authorized to make limited configuration changes system wide as approved by the VA Change Control Board.

h. **System Module Support** role holders are authorized to manage user accounts in VA-CABS application and execute user reports in the ADMIN module Import/Export. They also can review the import log if an issue is detected.