

**ATTACHMENT C: VA Directive and Handbook**  
**0710** *Personnel Suitability and Security Program*

## **PERSONNEL SECURITY AND SUITABILITY PROGRAM**

- 1. REASON FOR ISSUE:** This handbook establishes personnel security program responsibilities and procedural requirements for investigations, suitability adjudications, security clearance determinations, contractor fitness, and appeals of VA employees, appointees, volunteers, affiliates, health professions trainees and contractors set forth in Department of Veterans Affairs (VA) Directive 0710, Personnel Security and Suitability Program, June 4, 2010, in accordance with Title 5 Code of Federal Regulations (CFR) Part 731, Suitability, and 5 CFR 1400, Designation of National Security Positions.
- 2. SUMMARY OF CONTENTS/MAJOR CHANGES:** This handbook:
  - a. Clarifies changes to 5 CFR 731 regarding designation of Public Trust positions and reinvestigation requirements for Public Trust positions, procedures and information on reciprocity (accepting other agencies' favorably adjudicated background investigations) and fingerprint information based on Homeland Security Presidential Directive-12 (HSPD-12).
  - b. Introduces the Revised Federal Investigations Standards (FIS) 5 Tiered Investigations and National Training Standards for Suitability and National Security Adjudicators, as well as the changes to the designation of national security positions.
- 3. RESPONSIBLE OFFICE:** Office of Operations, Security and Preparedness, Personnel Security and Identity Management, Personnel Security and Suitability Service.
- 4. RELATED DIRECTIVE:** VA Directive 0710, Personnel Security and Suitability Program.
- 5. RESCISSIONS:** VA Handbook 0710, Personnel Suitability and Security Program, September 2004.

**CERTIFIED BY:**

/s/

LaVerne H. Council  
Assistant Secretary for  
Information and Technology

Distribution: Electronic Only

**BY DIRECTION OF THE  
SECRETARY OF VETERANS  
AFFAIRS:**

/s/

Kevin T. Hanretta  
Assistant Secretary  
for Operations, Security, and Preparedness

*Intentionally left blank*

## TABLE OF CONTENTS

1. INTRODUCTION AND APPLICABILITY .....	5
2. FEDERAL INVESTIGATIVE STANDARDS .....	8
3. DELEGATION OF AUTHORITY .....	9
4. RESPONSIBILITIES .....	10
5. POSITION DESIGNATION .....	13
6. POSITION SUBJECT TO INVESTIGATION .....	15
7. INVESTIGATION REQUIREMENTS.....	17
8. INTERIM SUITABILITY DETERMINATION/PRE-SCREENING.....	19
9. INVESTIGATIVE PROCESS.....	19
10. ADJUDICATION.....	26
11. CONTRACTORS.....	28
12. PERSONNEL ACTIONS AND RIGHTS OF EMPLOYEES .....	29
13. NATIONAL SECURITY ELIGIBILITY ACTIONS .....	32
14. SECURITY FILES AND INVESTIGATION RECORD.....	34
15. CHILD CARE EMPLOYEE BACKGROUND INVESTIGATIONS .....	36
16. PIV CARD INVESTIGATIONS AND ADJUDICATIONS.....	38
17. APPENDIX A (SENSITIVITY AND RISK LEVELS AND TIERS) .....	40
18. APPENDIX B (REFERENCES AND DEFINITIONS) .....	44
19. APPENDIX C (REVISED FIS AND 5 TIER MODEL).....	47
20. APPENDIX D (ACROYNMS) .....	48

*Intentionally left blank*

## PERSONNEL SECURITY AND SUITABILITY PROGRAM

### 1. INTRODUCTION AND APPLICABILITY

a. The purpose of this handbook is to establish and implement policy, procedures, provide guidelines, delegate authority, and assign responsibilities regarding personnel security, suitability, and fitness for personnel within the Department of Veterans Affairs (VA) pursuant to the authority of parts 302, 731, and 1400 of Title 5, Code of Federal Regulations (CFR). This handbook is applicable to VA employees, contractors, affiliates, volunteers, and health professions trainees.

b. VA is responsible for implementing a comprehensive and effective Personnel Security and Suitability Program (PSS). The PSS program:

(1) Evaluates the character and conduct of Government applicants and appointees for the purpose of making suitability determinations for covered positions and continuous evaluation through ensuring timely reinvestigations of employees in positions of public trust as required by *Executive Order (EO) 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Position of Trust*, and 5 C.F.R. part 731, Suitability.

(2) Evaluates the character and conduct of contractor employees by making fitness determinations for contractor employment per contractual requirements.

(3) Evaluates the character and conduct of Government employees for excepted service or other non-covered positions.

(4) Determines the eligibility of Federal employees for national security positions under *Executive Order 10450, Security Requirements for Government Employment*, the eligibility for access classified information under *Executive Order 12968, Access to Classified Information*; access to national security information and the issuance of a security clearance; continuous evaluation of individuals holding clearances; and 5 CFR 1400, *Designation of National Security Positions*.

(5) Determines the eligibility under Federal Information Processing Standards, (FIPS 201), "Personnel Identity Verification (PIV) of Federal Employees and Contractors" August 2008, and Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, for Personal Identity Verification for access to Federal facilities and Federally controlled information systems.

(6) To the extent consistent with standards and procedures set forth in regulations, laws,

and Executive Orders, policies and procedures relating to suitability and fitness for Federal employment shall:

(a) Provide for reciprocal recognition of existing investigations and favorable adjudications;

(b) Be cost-effective, timely, and provide efficient protection of the national interest; and provide fair treatment of those upon whom the Federal Government relies to conduct the Nation's business in accordance with:

1 Executive Order (EO) 10450 Security Requirements for Federal Employment April 27, 1953, as amended, in Reference (e);

2 EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to classified information June 30, 2008 in Reference (c);

3 EO 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals of Public Trust January 16, 2009 in Reference (d); and

4 Office of Personnel Management (OPM) and Office of the Director of National Intelligence (ODNI) Directives and policy issuances.

(7) Agency heads are directed by 5 CFR 731 to designate risk levels for positions in the competitive service and Senior Executive Service filled by career appointments. Risk levels are designated as Tier 4/High Risk, Tier 2/Moderate Risk, or Tier 1/Low Risk as determined by the position's potential for adverse impact on the integrity or efficiency of the service.

(8) Agency heads are directed by 5 CFR 1400 that all positions subject to investigation that could bring about an adverse effect on the national security or require access to classified information must also receive a sensitivity designation of Tier 5/Special-Sensitive, Tier 5/Critical-Sensitive, or Tier 3/Noncritical-Sensitive. This designation is in addition to the risk level determination and may have an impact on the position's investigative requirement.

(9) VA requires every applicant to be screened and/or a Tier investigation conducted based on the requirements of VA Policy, 5 C.F.R. 731 and 1400 and the risk and sensitivity level determined for that position, and if needed access to classified information.

(10) The appointment of an applicant or appointee to a covered position is subject to a suitability determination. Administrations making suitability determinations shall grant

reciprocal recognition to a prior favorable fitness or suitability determination unless a new investigation is required by EO 13467 or EO 13488.

(11) Title 38 and Title 38 Hybrid positions are also subject to an investigation and the adjudicative guidelines established by 5 CFR 731.

(12) Personnel filling positions as defined by 5 CFR 1400, Designation of National Security Positions, are subject to investigation and adjudication as established by EO 12968 and the Position Designation and Automation Tool (PDT).

(13) The Office of Operations, Security, and Preparedness; Personnel Security and Identity Management, Personnel Security and Suitability Service Program Management Office (PSSPMO) conducts oversight and functional program reviews to evaluate compliance and implementation of this Handbook.

(14) The OPM Position Designation Automated Tool (PDT) will be used to determine position risk and sensitivity levels and to identify the background investigation required for the position. Positions that are exempt from the requirements of EO 10450 are also exempt from the requirements of using the PDT.

(a) The PDT will also be used to determine the background investigation levels required for VA contract positions based on the terms of the contract.

1 Position descriptions should be evaluated for risk and sensitivity as part of the hiring process, prior to placement. If the PD has been modified, or position designation has not been conducted since the last review, an updated Position Designation Record (PDR) should be generated by the Servicing Human Resources Office (SHRO).

2 The PDT can be found at” [Position Designation Automated Tool](#)

(b) Adjudicative determinations, and any resulting actions, will be reported to OPM within 90 days of the close date of the investigation using the Clearance Verification System/ Personnel Investigations Processing System (CVS/PIPS).

(c) Information pertaining to suitability or fitness adjudications will be maintained in accordance with OPM policy.

(d) No negative inference may be raised solely on the basis of mental health counseling. Such counseling may be a positive factor that, by itself, shall not jeopardize the rendering of eligibility determinations or temporary eligibility for access to national security information. However, mental health counseling, where relevant to adjudication for a national security



position, may justify further inquiry to assess risk factors that may be relevant to the VA's Personnel Security Program.

(e) Discretionary judgments used to determine eligibility for national security positions are an inherently governmental function and shall be performed by appropriately trained and favorably adjudicated Federal government personnel or appropriate automated procedures.

(f) The VA shall not discriminate nor may any inference be raised on the basis of race, color, religion, sex, national origin, disability, or sexual orientation.

(g) No person shall be deemed eligible for a national security position merely by reason of Federal service or contracting, licensee, or grantee status, or as a matter of right or privilege, or as a result of any particular title, rank, position, or affiliation.

(h) No person shall be appointed or assigned to a national security position when an unfavorable personnel security determination has been rendered.

(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.

## **2. FEDERAL INVESTIGATIVE STANDARDS AND FIVE-TIERED INVESTIGATIVE MODEL**

a. Revised Federal Investigative Standards (FIS) established requirements for conducting background investigations to determine eligibility for logical and physical access, suitability for U.S. Government employment, eligibility for access to classified information or to hold a sensitive position, and fitness to perform work for or on behalf of the U.S. Government as a contractor employee.

b. The FIS align investigative elements at each tier to promote efficiency, consistency, and employee and contractor mobility across different governmental agencies thereby improving reciprocity and reducing program costs.

c. The standards at each level now build upon but do not duplicate each other. This ensures investigative requirements previously satisfied are not checked again just because an individual moves to a position requiring a higher level of investigation. The majority of VA positions are designated at Tier 1. The 5 tiers are as follows;

(1) **Tier 1:** Low Risk/Non-Sensitive Investigations conducted to this standard are for positions designated at low risk, non-sensitive, and for physical and/or logical access, pursuant

to Federal Information Processing Standards 201 and Homeland Security Presidential Directive-12, using Standard Form-85. This investigation is similar to the National Agency Check with Inquiries (NACI).

(2) **Tier 2:** Investigations conducted to this standard are for non-sensitive positions designated as moderate risk public trust, using Standard Form-85P. This investigation is similar to the Moderate Risk (MBI) background investigation.

(3) **Tier 3:** Non-Critical Sensitive Investigations conducted to this standard are for positions designated as non-critical sensitive, and/or requiring eligibility for “L” access or access to Confidential or Secret information. This is the lowest level of investigation acceptable for access to classified information, using Standard Form-86. Similar to the Access National Agency Check with Inquiries (ANACI) and the National Agency Check with Law and Credit (NACLC).

(4) **Tier 4:** Investigations conducted to this standard are for non-sensitive positions designated as high risk public trust, using Standard Form-85P. This investigation is similar to the Background Investigation (BI).

(5) **Tier 5:** Investigations conducted to this standard are for position designation as Critical Sensitive, Special Sensitive, and/or requiring eligibility for “Q” access or access to Top Secret or Sensitive Compartmental Information (SCI), using Standard Form-86. This investigation is similar to the Single Scope Background Investigation (SSBI).

### **3. DELEGATION OF AUTHORITY**

a. OPM has delegated to the Secretary of Veterans Affairs the authority to make suitability determinations and take suitability actions (including limited, agency-specific debarments) in cases involving applicants and appointees to covered positions in VA.

b. The Secretary of Veterans Affairs has delegated to the Assistant Secretary for Operations, Security, and Preparedness (OSP) the authority to maintain a personnel security and suitability program as authorized by laws, regulations, Executive Orders, and Directives.

c. Veterans Health Administration, Veterans Benefits Administration, and National Cemetery Administration will maintain responsibility for field operation of suitability programs within their respective organizations. Each Administration shall appoint a Personnel Security Program Manager to coordinate departmental regulations and policies involved with the overall personnel security and suitability program and to coordinate with the Personnel Security and Suitability Service.

d. OPM retains jurisdiction to make final determinations and take actions in all suitability cases where there is evidence that there has been a material, intentional false statement, or deception or fraud in examination or appointment. OPM also maintains jurisdiction over all suitability cases involving a refusal to furnish testimony.

e. OPM also retains jurisdiction to take suitability action against employees and to debar Government-wide.

#### 4. RESPONSIBILITIES

a. **Secretary of Veterans Affairs** has overall responsibility for VA's Personnel Security and Suitability Program, as directed in 5 CFR 731.103. The Assistant Secretary, Office of Operations, Security, and Preparedness is delegated the responsibility to implement and manage the program.

b. **Assistant Secretary for Operations, Security, and Preparedness (OSP)** will ensure the appropriate implementation and operation of this program through the Director, Office of Personnel Security and Identity Management (PS&IM). This includes, through the Deputy Assistant Secretary for Emergency Management and Resilience, establishing departmental standards for eligibility for access to classified information and sensitive but unclassified information and maintaining a central index of department-granted security clearances.

c. **The Director, Office of Personnel Security and Identity Management (PS&IM)** is responsible for developing, coordinating, and overseeing the implementation of policy, programs, and guidance for the VA's Personnel Security and Suitability Program. This includes but is not limited to:

(1) Developing departmental-wide personnel security and suitability policy, and conducting program oversight and reviews of VA Administrations and Staff Offices for implementation and compliance with VA personnel security policy and operating procedures.

(2) Developing a framework setting forth an overarching strategy identifying goals, oversight and assessment measures, roles and responsibilities, a communications strategy, training verification, and metrics to measure the quality of security investigations, suitability and fitness investigations and the corresponding adjudications, to ensure a sound VA personnel security program that will continue to meet the needs of VA per EO 13467.

(3) Recommending program enhancements through periodic evaluations and staff visits to ensure compliance with minimum Federal personnel security and suitability program standards.

- (4) Developing and maintaining a departmental wide Debarment Program.

**d. Assistant Secretary for Information and Technology (AS/OI&T).** The AS/OI&T will ensure the Office of Cyber Security develops and implements a Department wide Information System Security Program, commensurate with the Federal Information Security Management Act (FISMA), to protect information resources and to provide security measures commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of VA's information systems.

**e. Office of Inspector General (OIG).** The Inspector General Act of 1978 authorizes the OIG to select, appoint, and employ officers and employees subject to the provisions of Title 5, U.S.C. The OIG will coordinate, initiate, and adjudicate all background investigations for OIG employees in public trust and Tier 1/Low Risk positions.

**f. Assistant Secretary for Human Resources and Administration (AS/HR&A).** The AS/HR&A will collaborate with OSP to assist the Administrations and Staff Offices in maintaining an effective suitability program with timely adjudicative determinations.

**g. Under Secretaries, Assistant Secretaries, and Other Key Officials will:**

- (1) Comply with the policies, guidance and direction set forth in VA Directive 0710, Personnel Security and Suitability Program, and the procedures set forth in this Handbook.

- (2) Establish and maintain an effective suitability and fitness determination program using automated processes to the maximum extent practicable and taking actions to address and correct conditions that are non-compliant with the regulatory guidance.

- (3) Fund investigations required to determine eligibility for employment or continued employment. Fund investigations required to determine fitness eligibility for contractor-employees who perform work for, or on behalf of, VA.

- (4) Ensure an effective pre-investigative review (pre-screening) and adjudicative process within the organizational elements and ensure documentation is maintained and safeguarded in accordance with OPM guidelines.

- (5) Ensure establishment of criteria for utilizing interim suitability and fitness determinations based on initial investigatory results to the maximum extent practical based on mission requirements and position designation. Minimum criteria shall include a favorable fingerprint check, and other appropriate reviews, prior to the completion of the standard investigative requirements. Additional information is contained in the Pre-Screening (section 8) section of this Handbook.

(6) Ensure the appointment of individuals and their continued employment is consistent with the integrity and efficiency of the service and/or the interest of national security.

(7) Ensure encumbered positions are designated with the appropriate risk or sensitivity level in accordance with the PDT and ensure that each appointee and employee receives a background investigation commensurate with the position designation level. The position designation must also be recorded in Personnel and Accounting Integrated Data (PAID) HR Smart, or subsequent human resources information systems.

(8) Ensure position risk and sensitivity level designations are reviewed by appropriate Human Resources or Personnel Security officials to ensure that designations are consistently applied to all positions in accordance with 5 CFR Part 731, Suitability, and 5 CFR Part 1400, Designation of National Security Positions; and the VA information system security program and/or FISMA.

(9) When appropriate, refer appointees and employees in Public Trust and National Security positions to the Security and Investigations Center (SIC) for initiation and adjudication of the investigation. The use of the SIC's adjudication only product line enables servicing human resource offices to initiate their Public Trust investigations in e-QIP.

(10) Ensure a fingerprint Special Agreement Check (SAC) is conducted on all new appointees, employees, and affiliates who are exempt from the requirement to have a TIER 1/NACI or higher level investigation. Whenever possible, the SAC should be performed prior to the appointee's entrance on duty.

(11) Ensure the SAC is adjudicated by appropriately trained personnel expeditiously after the results are received. The SAC results must be recorded in CVS/PIPS.

(12) Administrations and Staff Offices acting under this delegated authority to adjudicate background investigations conducted on Federal employees must ensure the training of adjudicators 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). This training requirement can be met by successfully completing with a passing grade, the OPM Essentials of Suitability Adjudications Program (ESAP) course and/or the VA Suitability Adjudicator Training 201, when the training development is completed. In addition to meeting the National Training Standards adjudicators must have, at a minimum, a favorable background investigation based on the results of a Tier 4/High Risk level investigation.

**h. Office of Acquisition, Logistics, and Construction will:**

(1) Ensure appropriate language is included in applicable contracts so that the Statement of Work (SOW), Task Order, and/or Performance Work Statement accurately reflect the requirements of this directive and other applicable VA directives. The SOW (or other defining documentation related to the contract) must be reviewed using the PDT and given the appropriate position risk and sensitivity level designation.

(2) Ensure the necessary requirements are met for contractor background investigations and referred to the SIC for initiation and adjudication of the appropriate level of investigation. Failure to comply with background investigation requirements may result in a contractor being removed from VA facilities and denied a PIV credential.

(3) Ensure a SAC is completed on contractor employees and adjudicated at local facilities by a trained adjudicator, or at the VHA Service Center (VSC). Facilities may also utilize the SIC to review and adjudicate contractor SACs. Any SAC submitted to the SIC must be accompanied by a SAC Request Worksheet to ensure the COR or Program Manager is notified of the results. The SAC Request Worksheet can be found on the SIC's Resource Page.

**i. Information Security Officers (ISO)** will manage the local information security program and serve as the principal advisor regarding system access for users.

**j. Adjudicators** will:

(1) Evaluate pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether an individual is suitable and/or fit to work for or on behalf of the government.

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

(3) Be familiar with the laws, regulations, standards and criteria governing suitability adjudication.

## **5. POSITION DESIGNATION**

a. Proper position designation is the foundation of an effective and consistent personnel security and suitability program. Risk levels are designated as high, moderate, or low depending on the position's potential for adverse impact to the integrity or efficiency of the service. Positions at the high and moderate risk levels are public trust positions. Low risk

positions involve duties and responsibilities with the potential for limited impact on the integrity or efficiency of the service.

(1) All positions subject to investigation must be designated with a risk and sensitivity level based on the documented duties and responsibilities contained within the Position Description (PD) and based on the PDT review to determine the appropriate level of investigation for positions.

(2) Administrations and Staff Offices must ensure that human resources personnel receive sufficient training to be proficient at the task of assigning position risk and sensitivity designations. Only Human Resource Specialists and Personnel Security Specialists are authorized to determine position designation utilizing the PDT, with collaboration by the manager and/or supervisor (if warranted).

(3) The Program Manager/Contracting Officer/Contracting Officer Representative (collectively referred to as the COR in this handbook), in collaboration with a Personnel Security Specialist, designates contractor risk and sensitivity level for contractor positions required to fulfill the requirements of the contract and/or task order using the PDT.

(4) Risk levels are designated as Tier 4/High Risk, Tier 2/Moderate Risk, or Tier 1/Low Risk depending on the potential for adverse impact to the integrity or efficiency of the service.

(5) Positions at the Tier 4/High Risk and Tier 2/Moderate Risk levels are Public Trust positions.

(6) Tier 1/Low Risk positions involve duties and responsibilities with the potential for limited impact on the integrity or efficiency of the service.

(7) See Appendix A for an illustration of the Tiered Level Investigations and Risk levels.

(8) Sensitivity levels are designated Tier 5/Special-Sensitive, Critical-Sensitive, and Tier 3/Noncritical-Sensitive, depending on the potential for adverse impact to national security (including access to classified information). See Appendix A for an illustration of the sensitivity level designations.

(9) After risk and sensitivity designation, the PDT will produce the Position Designation Record (PDR). This PDR will be associated with each position description (PD) and copies will be maintained by the Servicing Human Resources Offices (SHRO) or the COR. Position designation data must be reflected in the PAID, HR Smart, or subsequent data systems for all VA employees.

b. Servicing Human Resources Office (SHROs), or appropriate designated officials, will:

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

(2) Ensure that adjudicative determinations are reflected in PAID, HR Smart, or subsequent data systems.

(3) Ensure careful review is taken place whenever an employee is moved from one position description (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.

## **6. POSITIONS SUBJECT TO INVESTIGATION**

a. Unless an exception exists elsewhere in this handbook, regulation, or law, the following positions are subject to investigation in VA:

(1) Covered positions, as defined by 5 CFR 731:

(2) Title 5 competitive service,

(3) Title 5 positions in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and

(4) Career appointments to the Senior Executive Service.

b. Additional positions subject to the provisions of 5 CFR 731:

(1) Title 5 excepted service,

(2) Title 5/Title 38 hybrid excepted service, and

(3) Employees appointed under 38 USC Chapters 3 (except the Under Secretary for Health), 71, and 78.

c. Additional positions subject to the criteria of 5 CFR 731: the Under Secretary for Health and employees appointed under 38 USC Chapters 73 and 74.



d. National security positions, as defined by 5 CFR 1400: positions with national security sensitivity in the competitive service and the Senior Executive Service where filled by career appointments.

e. Additional positions subject to the provisions of 5 CFR 1400:

(1) Title 5 excepted service,

(2) Title 5/Title 38 hybrid excepted service, and

(3) Employees appointed under 38 USC Chapters 3 (except the Under Secretary for Health), 71, and 78.

f. All positions requiring eligibility for access to classified information.

g. VA contractor positions performing duties under contract to VA in accordance with the terms of the contract.

h. A position may be subject to investigation under multiple authorities. Proper position designation is necessary to determine the correct investigation.

i. VA requested and received permission from OPM to exempt certain Tier 1/low-risk, non-sensitive positions from the investigative requirements of EO 10450, provided the VA conducts such checks as appropriate to ensure employment and retention are consistent with national security interests. This only applies to Tier 1/low-risk, non-sensitive positions. Personnel who are exempted from the investigative requirements of EO 10450 will be issued Non-PIV cards, instead of PIV cards. Exempt categories include:

(1) Intermittent, seasonal, per diem, or temporary, and

(2) Do not exceed an aggregate of 180 days per year in either a single continuous appointment or series of appointments.

(3) Without Compensation (WOC) healthcare practitioners who work for less than an aggregate of 180 days per year in either a single continuous appointment or series of appointments;

(4) Medical consultants who are appointed for 1 year or less and are not to be reappointed;

(5) Medical consultants who are appointed for more than 1 year or reappointed after 1 year with no break in service, but work less than 30 days per calendar year;

(6) Purchase and hire employees appointed for 6 months or less; and

(7) Employees appointed in either a single continuous appointment or series of appointments that do not exceed an aggregate of 180 days.

(8) Physicians appointed as medical residents are exempt from this requirement provided they do not exceed 1 year of continuous service at a VA facility, regardless of the durations of the residency program.

(9) Exemptions to investigation in this part do not change the Homeland Security Presidential Directive -12 (HSPD-12) minimum requirements for issuance of a PIV card, as opposed to a Non-PIV card. Affiliates who are required to receive a PIV card must meet the minimum investigative requirements for issuance of their PIV card which includes a favorable fingerprint check (SAC) and a favorable background investigation at the Tier 1/Low Risk - Non-Sensitive level. An employee does not have to serve a new probationary period solely because his or her appointment is subject to investigation.

## **7. INVESTIGATIVE REQUIREMENTS**

a. SHROs, or designated officials, must ensure the appropriate level and type of background investigation is requested and adjudicated to determine suitability or fitness for Federal employment of applicants and appointees to covered positions.

b. SHROs will, to the maximum extent practical, ensure that required investigations are initiated prior to appointment, if not prior, no later than 14 calendar days after entrance-on-duty (EOD).

c. The level of investigation required will be identified based on the results of the Position Designation System and Automated Tool (PDT) on the Position Designation Record.

d. Applicants shall be informed that their appointment is subject to the completion of a favorable suitability determination.

e. If the position is designated Tier 5/ Critical-Sensitive, the investigation should be completed before appointment. This requirement may be waived in case of an emergency by approval from the Deputy Assistant Secretary for Emergency Management and Resilience following a review of the e-QIP submission, Optional Form (OF) -306, and a completed SAC. The investigation must then be initiated within 14 days of the waiver.

f. If the position is designated Tier 5/Special-Sensitive, the investigation must be complete before placement. This requirement cannot be waived.

g. A change in position risk/sensitivity level requires a new background investigation at the required level. Reinvestigations and new investigations as a result of a position change (position designation modification) require the completion and submission of a new OF-306, Declaration for Federal Employment. In addition to the requirement of paragraph 7h below.

h. Within 14 days of the position risk or sensitivity level change, the SHRO or COR will submit the higher investigation request to the SIC, or the SHRO will initiate the case for an employee if using the adjudication only services offered by the SIC for employee background investigations.

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

j. The standards for suitability and national security are different; an investigation which satisfies one standard may not satisfy the other. A favorable suitability or fitness determination does not mean an individual is automatically eligible to hold a national security and/or sensitive position. A favorable national security adjudicative determination does not provide for automatic eligible to occupy a public trust or Tier 1/Low Risk position per 5 CFR 731.

k. 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 nor is a person who is qualified for a job automatically suitable for employment. Generally, suitability or fitness determinations are made after finding the person qualified for the position.

l. When an individual with a prior, favorably adjudicated investigation moves to a new position, either by a 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.

(4) No break in service of 24 months or more since the last investigation.

m. Post Appointment Arrest reports should be reviewed and adjudicated based on the employment status of the subject. For probationary appointees, reports should initially be reviewed by a trained Suitability Adjudicator for possible suitability action. For non-probationary employees, the reports should be referred to the local Employee Relations staff for possible adverse action.

## **8. PRE-SCREENING/INTERIM SUITABILITY DETERMINATIONS**

a. Part of an effective suitability and fitness determination includes pre-screening. An effective pre-screening process is essential to the identification and resolution of suitability or fitness issues early in the application process, prior to the initiation of the required investigation.

b. The pre-screening involves the review of applications, position description, and other employment related documents, the OF 306, Declaration for Federal Employment, as well as the results of the fingerprint Special Agreement Check (SAC).

c. SHROs shall use interim suitability determinations to the greatest extent practicable, based on the apparent absence of significant suitability issues using information from fingerprint checks, information on the OF-306, security forms, and investigative information available from OPM's CVS/PIPS.

d. The applicant may be presented with a tentative (conditional) employment offer when no derogatory information was identified in review of information provided by the applicant. In such cases, applicants will be informed that their appointment is subject to the completion of a favorable suitability or fitness determination. SHROs are encouraged to establish procedures to address, clarify, and potentially mitigate issues arising during the pre-employment process, prior to extending a firm offer of employment.

## **9. INVESTIGATIVE PROCESS**

### **a. Fingerprinting/Special Agreement Check**

(1) Every effort should be made to have applicants (new hires, contractors, and affiliates, etc.) fingerprinted prior to the applicant's entrance on duty (EOD). If this is not possible, fingerprints will be captured within 5 days of EOD.

(2) Fingerprint Special Agreement Checks (SACs) must be submitted to OPM electronically. The following information is required when submitting a SAC: Position/Occupation and reason for fingerprinting (PIV card issuance or background investigation) when fingerprinting Health Professions Trainees, use "Medical Trainee" in the Position/Occupation section.

(3) Employee SACs may be adjudicated by the SHRO or the Security and Investigations Center (SIC). Contractor SACs may be adjudicated by the facility submitting the SAC and/or the SIC. VHA contractor SACs may be adjudicated by the VHA Service Center (VSC).

(4) Care should be taken when adjudicating SACs for PIV purposes only. The OPM HSPD-12 Credentialing Criteria is to be used as the adjudicative methodology for PIV only SACs. Use the hyperlink to access OPM's Decision Making Guide:  
[http://www.opm.gov/investigate/resources/decision\\_making\\_guide.pdf](http://www.opm.gov/investigate/resources/decision_making_guide.pdf).

(5) SACs that result in a record must be adjudicated and the results recorded in CVS/PIPS. This is for all types, employees, contractors, affiliates and volunteers.

(6) Personnel with favorably adjudicated SACs do not require a new fingerprint screening unless:

(a) They are appointed to a new position that requires a higher level of background investigation (change in risk level), or;

(b) They require an initial PIV Credential Issuance.

(c) They require PIV Credential renewal during time of expiration (or for contractors, at the end of the Period of Performance or end of Contract).

(7) A new SAC is not required when:

(a) Issuing replacement PIV credentials (lost, stolen, damaged, or when an applicant has a name change).

(b) VA employees transfer within VA (inter-agency transfers) and shall not be taken unless (6) (a) above applies.

#### **b. Employee Tier 1/Low Risk/Non-Sensitive Positions**

(1) Every effort should be made to initiate new hires for their investigations using the OPM Electronic Questionnaire for Investigations Processing (e-QIP) prior to their EOD. Ideally, all pre-employment suitability documentation should be completely reviewed and submitted to OPM prior to granting a firm offer or arranging an EOD date. If not able to initiate/review e-QIP pre-EOD, SHROs will initiate the TIER 1/NACI or higher level investigation within 14 calendar days of an employee's appointment. If requested, SHRO may also utilize the SIC for their Tier 1/Low Risk/Non-Sensitive initiated and adjudicated. NOTE: Delays in background investigation submissions can also delay issuance of a PIV Credential.

(2) An appointee's background investigation shall be completed and suitability determination made within the first year of the appointee's service.

(3) Once the investigation has been completed and returned from OPM, the trained suitability adjudicator will review the report of investigation (ROI), using the OPM guidance, and make an adjudicative determination. Additional information regarding adjudication determinations is in section 10 of this handbook.

(4) Upon a favorable determination, the Certificate of Investigation (COI) is signed and a copy is placed in the employee's electronic Official Personnel Folder (e-OPF).

(5) The SHRO must record the decision in CVS/PIPS within 90 days of the closed date of the investigation.

(6) The adjudicative determination must also be entered into PAID or HR Smart as appropriate.

(7) The COI and Report of Agency Adjudicative Action (INV 79A) are retained locally.

(8) If the subject of an investigation separates or is no longer being considered for appointment, the investigation must be discontinued.

#### **c. Employee Tier 2/Moderate and Tier 4/High Risk/Non-Sensitive Positions**

(1) The SHRO may utilize the "Adjudication Only" service provided by the SIC and initiate Tier 2/Moderate and Tier 4/High Risk level investigations and review and release the case to OPM.

(2) The SHRO must send a complete investigation request worksheet, marked "Adjudication only," to the SIC to establish or update the individual's security file.

(3) Upon receipt of the ROI, the SIC will review and provide either a final adjudicative determination, or identify the actionable issues and forward the complete Report of Investigation (ROI), along with a summary of the issues, to the SHRO for review. Additional information regarding adjudications is in section 10.

(4) Prior coordination with the SIC is required for adjudication only requests.

(5) If the SHRO is not utilizing the "adjudication only" service of the SIC, the SHRO may submit a request to the SIC for Tier 2/Moderate or Tier 4/High Risk employee background investigations, within 5 days of the event that triggers the investigation (new hire, promotion,

etc.). Use the following website for investigation requests sent to the SIC:

<https://vaww.visn16.portal.va.gov/sites/lit/vasic/default.aspx>.

(6) The SIC will initiate the required investigation in e-QIP within five days of receiving a valid request and completed supporting documents. The SHRO and employee/appointee will be notified of the initiated investigation and provided instructions on the methods of completing the required background investigation.

(7) The employee must complete and release the e-QIP questionnaire, and provide all supporting documents, within five days of initiation notification. SHRO's should consider disciplinary, adverse or probationary actions for those who refuse to timely complete their investigation requirements. The SIC will review the completed e-QIP package and release the case to OPM or inform the employee and SHRO of any errors within five days of receipt of the completed e-QIP.

(8) The SIC will publish and maintain procedures for requesting background investigations for Tier 2/Moderate and Tier 4/High Risk positions within the VA.

**d. Employee Tier 3/Non-Critical Sensitive and Tier 5/Critical Sensitive National Security Investigations**

(1) Individuals in Tier 3 and Tier 5 (national security and or sensitive positions) who do not require access to classified information (eligibility only) are processed the same as Tier 2, and 4 level investigations as stated above in paragraph 9.c..

(2) Individuals in Tier 3 and Tier 5 level positions who require access to classified information cannot be initiated until the need for the access is validated. SHROs must follow their administration's internal guidance when submitting the following documents to the Special Security Officer (SSO), via the Operations and National Security Service (ONSS) to obtain the approval and validation:

- (a) Investigation Request
- (b) Justification for the Requested Security Clearance
- (c) Position Description
- (d) Position Designation Record
- (e) OF 306, Declaration for Federal Employment
- (f) Personal résumé

(g) Proof of current fingerprint check

(3) The SSO will review the requested package to ensure there is a valid need for access to classified information. The SSO will also review the position sensitivity level to ensure the PD is classified at the proper level. SSO will have 5 days from receipt of the request package to return it to the SHRO or forward it to the SIC. Upon receiving the complete investigation request, the SIC will initiate and process the investigation.

(4) SSO will notify the SIC when an employee no longer requires access due to a position change or separation from the VA. Upon notification, the SIC will remove the employee's national security access status from the OPM Central Verification System (CVS).

(5) The SIC will notify SSO when an employee requires a 5-year re-investigation (for National Security Clearances) at the 4 ½ year mark. All requests for reinvestigation of National Security Clearances (Top Secret, Secret, and Confidential) must be reviewed and approved by SSO to ensure all requirements are met to validate the position sensitivity levels. Any changes to an employee's access to classified information will be communicated to the SIC by the SSO. The SIC will remove the employee's clearance from OPM's Central Verification System. The SF-312 will be retained by the SSO.

(6) All persons who have access to classified information will complete an SF-312 Non-Disclosure Debriefing immediately upon leaving a position of access to classified information. The SSO will ensure that the signed SF-312 De-Brief is retained in SSO files.

**e. Contractor Investigations**

(1) 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 use of the Position Designation Tool.

(2) The investigation is required regardless of the location of the work. This includes contractor employees who use technology for remote access to VA facilities or VA information technology systems as well as those who have direct physical access to any VA data outside of any VA facility.

(3) The COR must submit a background investigation request and supporting documents for all contractors in Non-Sensitive positions to the SIC within five calendar days of the contract award. If the SIC cannot apply reciprocity for previously adjudicated background investigations, they will initiate the investigation within five days of receiving all required, complete documentation associated with the request. Administrations can develop their own internal



procedures for processing contractor investigations, but the final adjudication of contractor investigations must be determined by the SIC.

(4) The contractor will have five days to complete e-QIP and certify and release the required documentation to the SIC. After the contractor returns a complete, valid e-QIP package, the investigation will be submitted to OPM for processing within five days.

(5) Failure of the contractor to complete the background investigation process, to include e-QIP and submission of fingerprints and all required documents in a correct and legible form, will result in the revocation of access and removal of the specified noncompliant individual from the contract until such time as the background investigation is scheduled at OPM.

(6) VA is not currently a member of the National Industrial Security Program (NISP) and does not have the authority to enter into any national security classified contracts. Approval of any potential classified contracts must be made by the Director, Office of Operations and National Security.

#### **f. Child Care Workers**

(1) Child care workers must undergo a Childcare National Agency Check with Inquiries (CNACI). The CNACI includes state criminal history checks which are not normally included in the NACI.

(2) If the child care worker has been charged with a sex crime, an offense involving a child victim, a drug felony, or other crime bearing on the safety or well-being of children, the employer shall immediately restrict the worker's contact with children until the case is resolved. See Appendix B for additional information.

#### **g. Reinvestigations**

(1) Individuals Public Trust positions (Tier 2/Moderate Risk and Tier 4/High Risk) will be subject to reinvestigations at least once every five years. The SHRO or COR should request the reinvestigation within four months of the anniversary of the previous investigation's completion date. Prior to submitting the request (or initiating the investigation locally) the SHRO and COR must ensure the individual still occupies a position of public trust. The COR must also ensure the contractor is still working for or on behalf of VA prior to requesting the reinvestigation. Although the SHRO may initiate in e-QIP reinvestigations for Tier 2/Moderate and Tier 4/High Risk, the investigations must be adjudicated by the SIC. VA Police Officers occupy Moderate Risk positions and require a reinvestigation every five years.

(2) Individuals in a national security position requiring eligibility for access to classified information are subject to the reinvestigation requirements of Executive Order 12968 in Reference (f). As of the publication date of this Handbook, Individuals in Critical-Sensitive or Special-Sensitive designated positions require reinvestigations at least once every 5 years from the previous investigation's closed date.

(3) A reinvestigation must be conducted if the position requirements change to reflect a higher level of risk or sensitivity level. If the subject of a reinvestigation is an employee as defined by 5 U.S.C section 7511, and if a suitability issue is raised in a reinvestigation, the agency may elect to initiate an adverse action under part 752 of Reference (b), which is distinct from a suitability action under the procedures of part 731 of Reference (b).

(4) Any issues discovered in a reinvestigation must be evaluated to determine whether a person's continued employment promotes the efficiency of the service.

#### **h. Reciprocity**

(1) SHROs or appropriate designated officials will ensure, except as otherwise excepted by law, that acceptance of prior suitability or fitness determinations, background investigations, and adjudications shall be reciprocally accepted in accordance with References (b) and (c). As with any background investigation request, a check of CVS/PIPS will be done to review if a previous investigation has been completed and adjudicated. If the investigation has not been favorably adjudicated within the previous 24 months, the case may be ordered by either the SHRO or the SIC, as appropriate, for review and adjudication. Cases older than 24 months should not be used and a new case should be initiated.

(2) Reciprocal recognition of favorable suitability or fitness determinations should be applied when:

(a) The gaining agency uses criteria for making fitness determinations equivalent to suitability standards established by the OPM;

(b) The prior favorable fitness or suitability determination was based on criteria equivalent to suitability standards established by the OPM.

(3) The individual has not had a break in Federal service of 24 months or more since the favorable determination was made.

(4) Reciprocal recognition of a prior favorable fitness or suitability determination is not required when:

(a) The new position requires a higher level of investigation than previously conducted for that individual;

(b) The agency obtains new information that calls into question the individual's fitness based on character or conduct; or

(c) The investigative record shows conduct that is incompatible with the core duties of the new position.

(5) SHROs apply reciprocity in cases of Tier 1/Low Risk/Non-Sensitive employees, and complete VA Form 4236, Certificate of Eligibility/Reciprocity, and retain a copy in the employee's E-OPF. This information must also be entered into the PAID system. Public trust employees may be reviewed for reciprocity by the SHRO as long as no identified issues are present (OF-306, SAC, etc.) in which case reciprocity is not applicable and a new investigation is required. Contractors will be processed through the Security and Investigations Center (SIC), which will determine if reciprocity applies. Reciprocity requests made to the SIC for positions of public trust, must submit the OF-306 and position description for the new position to ensure no issues arise that may have a connection to the requested position.

(6) Reciprocity is based on final determinations. If there is no adjudicative information or basis available (PIPS or by contacting OPM directly) the SHRO and/or the SIC may request the investigative file for review to assist in making a suitability or fitness determination.

## **10. ADJUDICATION**

a. Adjudicators must also be trained in accordance with the OPM National Training Standards for Suitability Adjudicator Guidelines. Suitability or fitness determinations are based on careful, objective analysis of information about a person's character and conduct, both favorable and unfavorable, that is relevant to the criteria set forth in 5 CFR 731. The position and sensitivity level are also considered when making suitability or fitness determinations. Adjudicators must have been subject to a favorable determination of at least a Tier 4/High Risk/Background Investigation (BI).

b. VA works with many individuals who do not require a suitability determination, but they need an investigation to obtain a PIV credential. In such cases, the OPM's Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, dated July 31, 2008, and are used, in addition to the basic standards, when adjudicating the closed investigation. The supplemental standards are intended to ensure that the granting of a PIV credential to an individual does not create an unacceptable risk, when the individual is not

subject to an adjudication of suitability for employment in the competitive service under 5 CFR 731.

c. A review of the report of investigation is performed to identify actionable issues in accordance with the suitability factors to make an assessment of those issues. Information is analyzed in terms of its relevancy, nature and seriousness of the conduct, circumstances surrounding the conduct, recency of the conduct, the age of the person at the time of the conduct, contributing societal conditions, 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 (see Table 2 , Additional Suitability Considerations).

d. Suitability determinations shall be made using 5 CFR 731 and OPM's supplemental guidance as described in Reference (i).

e. The objective of the Adjudicator is to establish a reasonable expectation that employment or continued employment of the person either would or would not protect the integrity or promote the efficiency of the service. When there is reasonable expectation a person's employment would not do so, the person must be found unsuitable. This expectation is established when an adverse nexus or connection can be shown between the character or conduct in question and the integrity of a competitive examination or appointment, the integrity of the competitive examining system, or the person's capacity and fitness for employment in covered positions. Protecting the interests of the Federal Government is the first responsibility of the Adjudicator.

f. Adjudicative actions are to be reported to OPM using CVS/PIPS. SHROs, or appropriate designated officials and must maintain a copy of final adjudication actions (Certificate of Investigation (COI), INV 79A, suitability worksheet, and case notes).

g. In suitability cases where there is evidence of material, intentional false statement; or deception or fraud in examination or appointment; or a refusal to furnish testimony the suitability adjudicator must refer the case to OPM.

h. SHROs are required to record all final adjudicative actions with OPM. Actions based on an OPM investigation must be recorded as soon as possible and not later than 90 days from the close date of the final report of investigation with OPM.

i. In the case of unfavorable adjudication, follow the processes described in Personnel Actions and Rights of Employees in this handbook.

j. National security eligibility determinations and determinations of eligibility to access classified information are based on an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable risk to national security.

k. The SIC will adjudicate national security and sensitive level investigations.

l. Adjudicative actions, including the granting of a security clearance if applicable, are recorded to OPM using PIPS/CVS. The SIC will maintain a copy of the final adjudication actions (COI, INV 79A, issue worksheet, and case notes) and, if a clearance is granted, the SF 312. If the adjudicative process indicates the clearance should be denied or revoked, one of the processes described in Actions, "National Security Eligibility Actions" will be used.

m. VA will not discriminate nor may any inference be raised on the basis of race, color, religion, sex, national origin, disability, or sexual orientation.

n. Discretionary judgments that determine eligibility for national security positions shall be clearly consistent with the national security interests of the United States. Any doubt shall be 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, or as a matter of right or privilege, or as a result of any particular 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.

o. Eligibility for national security positions shall be granted only to persons who are U.S. citizens for whom the investigative and adjudicative process has been favorably completed. However, based on exceptional circumstances where official functions must be performed prior to completion of the investigative and adjudicative process, temporary eligibility for access to classified information may be granted while the investigation is underway.

## **11. CONTRACTORS:**

(1) All contractor fitness determinations within the VA will be conducted by the SIC. Contractor fitness determinations will be performed in the same manner as employee determinations, using the suitability criteria of 5 CFR 731. VA reserves the right to restrict access to VA facilities, sensitive information, or resources, for any contractor.

(2) A contractor on whom unfavorable or derogatory information has been discovered or detected during a personnel investigation will be so advised by the SIC and offered an opportunity to refute, explain, clarify, or mitigate the information in question.

(a) The individual should also be advised that the VA will not disclose any details of the adverse information to the contractor's firm.

(b) After final adjudication of unsuitable or unfavorable information on an individual working on a contract the SIC will notify the individual and the COR. The Contracting Officer (or COR if authorized to communicate with the contractor employee's employer under this circumstance) must communicate to the employer (contract company) that:

1 The contractor personnel 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 suitability for employment elsewhere in the company is in any way affected by the VA determination on access to VA facilities or information.

## **12. PERSONNEL ACTIONS AND RIGHTS OF EMPLOYEES**

a. SHROs shall ensure that suitability actions are handled in accordance with the procedural requirements in part 731 of Reference (b). Actions taken based on conduct issues that may also be suitability concerns are handled in accordance with the procedural requirements in parts 315 (appointees), 359 (SES), or 752 (employees), of Reference (b).

b. A suitability action is an outcome taken by OPM or an employing activity following an unfavorable suitability determination under the procedures of part 731 of Reference (b). Suitability actions are:

(1) Cancellation of eligibility

(2) Removal

(3) Cancellations of reinstatement eligibility, and

(4) Debarment.

c. SHROs may submit debarment requests for up to three years from the date of the unfavorable suitability determination for all, or specific covered positions in accordance with part 731 of Reference (b). Agencies do not have the authority to bar from all covered positions Government-wide. Any proposed debarments must be approved by PSS and accessible to all VA stations prior to the debarment becoming effective. Debarment requests should be routed to PSS for approval according to internal administration processes.

d. Suitability actions may be taken against applicants and appointees in covered positions, and applicants and appointees in positions to which VA has extended the provisions of part 731 of Reference (b). Suitability criteria may also be used as the basis of adverse action under other applicable regulations. The procedures in this section do not apply to contractor personnel.

e. Title 38 Health Care Applicants, Appointees, and Employees (including the Under Secretary for Health). Suitability determinations and procedural protections for applicants, appointees, and employees appointed under 38 USC § 7306, § 7401(1), § 7405, and § 7406, and the Under Secretary for Health, are outlined in VA Directive and Handbook 5021, Employee/Management Relations. Separations based on suitability criteria will be subject to the separation procedures outlined for the various types of appointments.

f. Applicants and appointees:

(1) OPM has delegated limited authority for adjudicating suitability for applicants and appointees in covered positions. OPM retains jurisdiction over all covered positions when there is evidence of material, intentional false statement, deception, fraud in examination or appointment, and refusal to furnish testimony required by 5 CFR § 5.4. VA must refer these cases to OPM for adjudication.

(2) Although no prior approval is required, notification to OPM is required if the agency wants to take, or has taken, action under its own authority (5 CFR 315, 5 CFR 359, or 5 CFR 752) in cases involving:

(a) Material, intentional false statement in examination or appointment, or deception or fraud in examination or appointment or

(b) Refusal to furnish testimony as required by 5 CFR § 5.4.

(3) OPM may assume jurisdiction in any case it deems necessary. Pass over requests involving preference eligible individuals who are 30 percent or more compensable disabled, and medical pass overs of preference eligible or disabled veterans in certain circumstances (5 CFR 339), must be referred to OPM.

g. VA does not have delegated authority to take a suitability action against an employee past their probationary period (employee as defined in part 731 of Reference (b)). However, VA is not precluded from taking an action against an employee under the procedures set forth in part 752 and 315 of Reference (b), based on suitability criteria.

h. When OPM instructs VA to take a suitability action against an applicant, appointee or employee, the following procedures, will be followed:

(1) OPM will inform the respondent of the Proposed Action through mail to the SHRO/Security Office Identifier (SOI) requesting the investigation.

(2) The correspondence will be hand delivered or certified mailed to the respondent in a sealed envelope.

(3) A separate copy of this notice will be sent to the SOI for their records.

(4) The Proposed Action Letter (PAL) will be presented to the respondent who will sign the provided receipt.

(5) This receipt will be returned to OPM's Suitability Branch via the fax number provided on the instructions, or by the OPM Secure Portal.

(6) This Proposed Action Letter (PAL) will instruct the respondent of the charges against them and the timeframe the respondent has to reply.

(7) It will also inform the respondent of their right to be represented by counsel or other representative at their own expense, and to request the entire investigative file or any documents, records, and reports upon which the suitability action was based. The representative must be designated by the respondent in writing.

(8) If OPM determines removal is the suitability action to be taken, they will inform the respondent, and notify the VA to remove the individual from the rolls within 5 days of receipt of OPM's final decision. After removal, the SHRO should code the removal using Rule 54 from the guide to processing personnel actions.

i. If VA initiates a suitability action against an applicant or appointee, then the procedures specified in part 731 of Reference (b) must be followed.

(1) The VA must notify the applicant or appointee (hereinafter, the "respondent") in writing of the proposed action, the charges against them and the availability of information relied upon request by the respondent.

(2) The notice must set forth the specific reasons for the proposed action and state that the respondent has the right to answer the notice in writing.

(3) The notice must further inform the respondent of the time limit for the answer as well as the mailing address to which such answer should be delivered.



j. The respondent of the proposed action will receive notice of the right to be represented by counsel or other representative at their own expense, and to request the entire investigative file or any documents, records, and reports upon which the suitability action is based.

k. VA must serve the notice of proposed action upon the respondent by mail or hand delivery no less than 30 days prior to the effective date of the proposed action to the respondent's last known residence or duty station.

(1) If the respondent is employed in a covered position on the date the notice is served, the respondent is entitled to be retained in a pay status during the notice period.

(2) The respondent may respond to the charges in writing and furnish documentation and/or affidavits in support of the answer. The respondent must submit the written response no more than 30 days after the date of the notice of proposed action.

(3) The decision regarding the final action must be in writing and inform the respondent of the reasons for the decision and that an unfavorable decision may be appealed to the Merit Systems Protection Board (MSPB).

l. The SHRO must remove an appointee from the rolls within five workdays of the final determination which requires removal.

m. Office of the Inspector General (OIG) takes a suitability action under its delegated authority for applicants or appointees in the OIG.

n. Adverse actions based on an OPM investigation, whether under part 731 of Reference (b) or VA's own authority, must be reported to OPM as soon as possible but no later than 90 days after receipt of the investigative report.

### **13. NATIONAL SECURITY ELIGIBILITY ACTIONS**

a. National Security positions requiring security clearances are limited at VA. However, when VA makes an adjudicative national security eligibility determination based on an OPM investigation, or when VA, as a result of information in an OPM investigation, changes a tentative favorable placement or clearance decision to an unfavorable decision, it must provide the minimum due process protections and appeal rights that are contained in part 731 of Reference (b).

b. At a minimum, VA must provide the individual with notice of the specific reason(s) for the decision, an opportunity to respond, and notice of any appeal rights. VA also must ensure that the records used in making the decision:

(1) Are accurate, relevant, timely, and complete to the extent reasonably necessary to ensure fairness to the individual;

(2) Comply with all applicable administrative due process requirements, as provided by law, rule, or regulation;

(3) Consider all available information in reaching its final decision; and keep any record of the agency action required by OPM.

c. Under 5 USC 7532(a), the Secretary or designee may suspend an employee without pay when that action is necessary in the interests of national security.

(1) To the extent the Secretary or designee determines the interests of national security permit it, the suspended employee must be notified of the reasons for the suspension.

(2) Within 30 days after the notification, the suspended employee is entitled to submit statements or affidavits to show why duty status should be restored.

d. The Secretary or designee may remove a suspended employee when, after such investigation and review as the Secretary considers necessary, it is determined that removal is in the interests of national security. Before removal, the employee is entitled to the reply, hearing, and review procedures of 5 USC 7532(c). The Secretary's determination is final.

e. Where an employee has lost a security clearance that is required for the position, VA may take adverse action against the employee for "cause" under 5 USC 7512-7513 or subchapter 5 of 38 USC Chapter 74, as applicable.

(1) Employees are entitled to the procedural protections of 5 USC 7513, including appeal to the MSPB, and VA Directive and Handbook 5021, Employee/Management Relations, as applicable. These procedural protections apply only to the adverse action.

(2) An employee wishing to dispute the merits of the security clearance determination itself may do so according to the procedures in the following paragraph.

f. A security clearance may be denied or revoked when it is determined an employee does not meet the standards of the Adjudicative Guidelines of Reference (I). Due process must be provided to applicants, employees, and contractors pursuant to Reference (I).

g. VA will provide a written explanation of the basis for the denial or revocation that is as comprehensive and detailed as the national security interests of the United States and other applicable law permit.

h. The subject of the proposed revocation action will receive notice of the right to be represented by counsel or other representative at their own expense, and to request the entire investigative file or any documents, records, and reports upon which the denial or revocation is based.

i. If requested by the subject of the proposed revocation action, any documents, records, and reports upon which the denial or revocation is based must be provided within 30 days, to the extent permitted by national security and applicable laws, and the entire investigative file must be provided prior to the time set for a written reply. The subject must receive a reasonable opportunity to review the determination and reply in writing.

j. The subject must receive written notice of the results of the review, the identity of the deciding authority, and written notice of the right to appeal.

k. The subject will have the opportunity to appeal in writing to a high level panel (Security Appeals Board/SAB), appointed by the Secretary, which must comprise at least three members, two of whom must be selected from outside the security field. The decision of the appeals panel must be in writing, and will be final, except where the Secretary personally exercises the appeal authority based upon recommendations from the appeals panel. In such case, the decision of the Secretary will be final.

#### **14. SECURITY FILES AND INVESTIGATION RECORDS**

a. Personally Identifiable Information (PII) in personnel security investigations, records, and operations shall be carefully safeguarded to protect the interests of both the individual and the VA, pursuant to requirements of the Privacy Act of 1974.

b. Security files must be stored in locked cabinets (if not electronic). All documentation must be maintained, at a minimum, of two years.

c. SHROs will establish and maintain security files for all their employees in Tier 1/Low Risk positions. If the SHRO is utilizing the adjudication only service for Tier 2 and Tier 4 investigations, the SIC will maintain the security file on employees and return the Certificate of Investigation on completed investigations. The SHRO will ensure PAID is updated on employees who occupy Public Trust positions. The security files can be stored electronically instead of the traditional hard copy folders. The electronic security files must contain all the

required information from the Report of Investigation (ROI). The security files will contain (as appropriate):

- (1) Case Closing Transmittal (CCT),
- (2) Certificate of Investigation (COI) or Certificate of Eligibility (COE),
- (3) Report of Agency Adjudicative Action (INV Form 79A\79C-Unless case received electronically),
- (4) Suitability Worksheet, and
- (5) Any derogatory information developed or received in the course of the investigation.

d. The SIC will establish and maintain personnel security files for employee background investigations at the Tier 2/Moderate and Tier 4/High Risk levels (VA-wide employees), and for contractors at all investigative types. The SIC's security files will contain (as appropriate):

- (1) CCT,
- (2) COI or COE,
- (3) INV Form 79A,
- (4) Suitability Worksheet, and
- (5) SF 312, Classified Information Nondisclosure Agreement.

e. If derogatory information on an individual who occupies a national security or public trust position becomes known to the facility's SHRO, the SHRO will notify the SIC in writing. The SHRO should be notified in writing of derogatory information from any other individual to include VA management officials or VA law enforcement officials. The SHRO must make a reasonable effort to ensure the information is accurate prior to notifying the SIC, who will review the information to determine the appropriate action.

f. Likewise, if derogatory information on a contractor becomes known to a COR (or other VA contractor or employee and disclosed to the COR or a VA employee), that COR will notify the SIC in writing.

(1) The COR should be notified in writing of derogatory information from any other individual to include VA management officials, contractor company management, or VA law enforcement officials.

(2) The COR must make a reasonable effort to ensure the information is accurate prior to notifying the SIC, who will review the information to determine the appropriate action.

g. The VA does not distribute investigative reports outside of offices with adjudicative functions. The subject of an investigation may request a copy of their investigation from OPM. Directions for obtaining one's report are on the OPM Federal Investigative Services web site (<https://www.opm.gov/investigations>).

## **15. CHILD CARE EMPLOYEE BACKGROUND INVESTIGATIONS**

a. All child care centers operating under a lease agreement on the Department of Veterans Affairs (VA) property are required to comply with Federal background investigations and state criminal history repository checks to ensure the safety and security of children, VA staff, Veterans, volunteers and visitors to the VA facilities.

b. Federal statutes require criminal history background checks on all individuals associated with providing child care services to children under the age of 18. Specifically, Public Law No. 101-647, Section 231 and Public Law No. 102-190, Section 1094 define procedures applicable for existing and newly hired child care facility personnel. In addition, these statutes require a review of personnel and security records to include a Federal Bureau of Investigation (FBI) fingerprint check and State Criminal History Repositories (SCHR) checks of residences listed on employment or certification applications.

c. In response to the specific requirements within Public Law 101-647 and Public Law 102-190 for criminal background checks for child care center workers to include both a check of FBI data bases as well as State Criminal History Records Checks, the Office of Personnel Management (OPM) created the Federal background investigation product specifically to support Child Care Provider Investigations. Federal Investigations Notice Letter 97-05, dated August 19, 1997 describes the investigative product line, exclusively intended for child care provider positions. The Child Care National Agency Check with Written Inquiries (CNACI) was designed by a consortium of Federal agencies which offer child care services. The scope of the CNACI includes the basic National Agency Check with Written Inquiries (Tier 1/NACI) and state criminal history repository (SCHR) checks for all states of residence. The CNACI meets the intent of the Crime Control Act of 1990, P.L. 101-647 Section 231.

d. OPM assesses VA and other Federal Government Agencies a standard fee for the CNACI, a processing fee for each SCHR search conducted, and the additional user fee charged by each state, if any.

e. Public Law 101-647 states that any conviction for a sex crime, an offense involving a child victim, or a drug felony, may be grounds for denying employment or for dismissal of any

employee at a child care center. The law allows agencies to suspend an employee from having any contact with children while on the job in the case of an offense when the charge has not been disposed of as listed above. Conviction of a crime other than a sex crime may be considered if it bears on an individual's fitness to have responsibility for the safety and well-being of children at VA child care centers.

f. Employment applications used by the child care center provider that operates or maintains child care services at a VA facility, must have specific language related to crimes involving a child. The employment applications for individuals who are seeking work shall contain a question asking whether the individual has ever been arrested for or charged with a crime involving a child, and if so, requiring a description of the disposition of the arrest or charge. The application shall state that it is being signed under penalty of perjury, with the applicable Federal punishments for perjury stated on the application. Applications must also state the requirement for employees to report all arrests, post-employment, for charges involving children.

g. The child care center may hire staff provisionally prior to the completion of a background check. However, the provisional employee may never be alone with children under her/his care and must at all times in the presence of children be physically supervised by an employee of the child care center who has successfully completed a CNACI investigation.

h. All employment or volunteer positions are strictly contingent upon a favorable adjudicative determination of their background investigation to meet fitness and suitability requirements in compliance with the Crime Control Act of 1990. Individuals must be advised that disqualifying derogatory information will result in refusal of employment. Applicants have a right to obtain a copy of the criminal history report and to challenge the accuracy and completeness of any information contained in the report.

i. Within 14 calendar days of the issuance of this Handbook, all current child care center employees, contractors and volunteers at VA facilities will be initiated for the CNACI level investigations, which includes SCHR, and every year thereafter throughout the duration of their employment or lease, whichever terminates first.

j. New Employees, Contractors and Volunteers

(1) Newly-hired employees, contractors and volunteers must undergo a criminal history background check at the CNACI level.

(2) Background investigations will be coordinated through the servicing human resources office with the assistance of the child care center director. The SHRO will process, review, and adjudicate all CNACI level investigations. The SHRO may also chose to utilize the SIC to process and adjudicate these cases using the "adjudication only" service.

(3) Current Employees, Contractors and Volunteers: Current employees will have 14 days, from the issuance of this Handbook, to complete the investigative requirements of initiating the CNACI. All persons employed or volunteering at a child care center at a VA facility must receive a favorable adjudicative determination from a CNACI to meet fitness and suitability requirements for employment in compliance with the Crime Control Act of 1990. The servicing HR Office will process, review, and adjudicate all CNACI level investigations. If derogatory information is reported regarding an employee, contractor, or volunteer, the individual will be given the opportunity to request a copy of the criminal history report and challenge the accuracy and completeness of the information before formal personnel action is taken.

(4) Employees must be advised that any disqualifying derogatory information will result in refusal of employment. Employees, contractors, and volunteers determined to be unsuitable to provide child care services will be removed from employment, escorted off VA facilities, and barred from working with children at any other VA child care center.

## **16. PIV CARD INVESTIGATION AND ADJUDICATION**

a. A favorably adjudicated National Agency Check with Inquiries (NACI)/Tier 1 or equivalent is the minimum investigation required for a final credentialing determination of a PIV credential. Individuals requiring a PIV credential must meet the credentialing standards in accordance with the Office of Personnel Management's Final Credentialing Standards Issuance, July 2008. Individuals with a statutory or regulatory bar are not eligible for reconsideration while under debarment.

b. Discretionary judgments used to render an adjudicative determination for issuing the PIV are inherently governmental functions and must only be performed by trained U.S. Government personnel who have successfully completed required training.

c. Favorable credentialing adjudications from another federal department or agency will be reciprocally accepted. Reciprocity must be based on final favorable adjudication only.

d. Individuals identified as having a favorably adjudicated investigation on record, equivalent to or greater than the NACI, do not require an additional investigation for PIV issuance. All investigations and adjudications required for non-VA personnel are for current, active contracts or other agreements and that the number of personnel submitted for investigation and adjudication does not exceed the specific requirements of that contract or agreement while ensuring compliance with HSPD-12.

e. There is no requirement to reinvestigate VA PIV holders unless they are subject to reinvestigation for national security or suitability reasons as specified in applicable VA policy. However, VA policy does require a new SAC at the issuance and reissuance of a PIV card.

f. The PCI Facilities must not re-adjudicate PIV determinations for individuals transferring from another VA facility or federal department or agency, provided:

(1) The individual has undergone the required NACI or other equivalent (or greater) suitability or national security investigation and received favorable adjudication from the former department or agency.

(2) There is no break in service 2 years or more and the individual has no actionable information since the date of the last completed investigation.

g. Guidance For Applying Credentialing Standards During Adjudication

(1) HSPD-12 credentialing standards must be used to render a final determination whether to issue or revoke a PIV card based on results of a qualifying investigative type. Credentialing adjudication considers whether or not an individual is eligible for long-term access to federally controlled facilities and/or information systems. The ultimate determination to authorize, deny, or revoke the PIV card based on a credentialing determination of the PSI must be made after consideration of applicable credentialing standards.

(2) **Basic Standards.** PIV credentialing standards and the adjudicative guidelines are designed to guide the adjudicator who must determine, based on results of a qualifying investigative type, whether PIV issuance is consistent with the basic standards, would create an unacceptable risk for the U.S. Government, or would provide an avenue for terrorism.

(3) **Supplemental Standards.** The supplemental standards are intended to ensure that the issuance of a PIV to an individual does not create unacceptable risk. The supplemental credentialing standards must be applied, in addition to the basic credentialing standards. In this context, an unacceptable risk refers to an unacceptable risk to the life, safety, or health of employees, contractors, vendors, or visitors; to the Government's physical assets or information systems; to personal property; to records, including classified, privileged, proprietary, financial, or medical records; or to the privacy of data subjects. The supplemental credentialing standards, in addition to the basic credentialing standards, must be used for PIV adjudication of individuals who are not also subject to the following types of adjudication:

(a) Eligibility to hold a sensitive position or for access to classified information,

(b) Suitability for federal employment in the competitive service, or

(c) Qualification for federal employment in the excepted service.



## Appendix A. Sensitivity and Risk Levels and Tiers

**Table 1: Position Sensitivity/Tiers**

SENSITIVITY LEVEL	CRITERIA
Tier 5/ Special-Sensitive	<p>Positions with the potential to cause inestimable damage to the national security, including:</p> <ul style="list-style-type: none"> <li>• Access to Sensitive Compartmented Information (SCI)</li> <li>• Access to any other intelligence-related Special Sensitive information or involvement in Top Secret Special Access Programs (SAP)</li> <li>• Any other position the agency head determines to be at a higher level than Critical-Sensitive due to special requirements that complement EO 10450 and EO 12968</li> </ul>
Tier 5/ Critical-Sensitive	<p>Potential for exceptionally grave damage to the national security. Includes positions involving any of the following:</p> <ul style="list-style-type: none"> <li>• Access to Top Secret or “Q” classified information</li> <li>• Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.</li> <li>• National security policy-making or policy-determining positions, the duties of which have the potential to cause exceptional or grave damage to the national security</li> <li>• Investigative duties, the issuance of personnel security clearances, or duty on personnel security boards</li> <li>• The adjudication, recommendation of adjudicative determinations, and/or granting of personnel security clearances</li> <li>• Duty on personnel security boards</li> <li>• Other positions related to national security, regardless of duties, that require the same degree of trust.</li> </ul>
Tier 3/ Noncritical-Sensitive	<p>Potential for damage to the national security. Includes positions that involve any of the following:</p> <ul style="list-style-type: none"> <li>• Access to Secret, “L,” or Confidential national security information</li> <li>• Duties that may directly or indirectly adversely affect the national security operations of the agency and do not rise to the level of the positions listed above.</li> </ul>
Non-Sensitive	All other positions not designated as Sensitive

**Table 2: Position Risk Levels/Tiers**

<b>RISK LEVELS</b>	<b>CRITERIA</b>
Tier 4/ High Risk Public Trust	<p>Positions included are those that have the potential for exceptionally serious impact involving duties especially critical to the agency or a program mission with broad scope of policy or program authority:</p> <ul style="list-style-type: none"> <li>• Policy making, policy determination, and policy implementation</li> <li>• Assignments with major program or line management responsibilities (for example, Senior Executive Service (SES) positions or SES equivalents)</li> <li>• Independent spokesperson or non-management positions with authority for independent action</li> <li>• Other positions designated by the agency head or designee that require the same degree of Public Trust</li> </ul>
Tier 2/ Moderate Risk Public Trust	<p>Positions included are those that have the potential for Tier 2/moderate to serious impact involving duties of considerable importance to the agency or program mission with significant program responsibilities and delivery of customer services to the public such as:</p> <ul style="list-style-type: none"> <li>• Senior staff assistants to positions with policy making, determining and implementation authority</li> <li>• Mid-level management assignments such as supervisory or managerial positions that report directly to an SES position or SES equivalent</li> <li>• Non-management positions with authority for independent or semi-independent action</li> <li>• Other positions designated by the agency head or designee that require the same degree of Public Trust</li> </ul>
Tier 1/ Low Risk	<p>Potential for impact involving duties of limited relation to the agency mission with program responsibilities that affect the efficiency of the Federal service. Computer positions not included in the criteria for Public Trust levels.</p>

**Federal Investigative Standards (FIS) Crosswalk**

<b>For this Position Designation and Risk/Sensitivity Level:</b>	<b>Use This Standard Form:</b>	<b>Prior Investigations:</b>	<b>Revised Investigations and Implementation Dates:</b>
<b>Non-Sensitive Position</b> <b>(Low Risk/HSPD-12 Credential)</b> <b>(No national security sensitivity)</b>	SF 85  (Questionnaire for Non-Sensitive Positions)	National Agency Check and Inquiries (NACI)  *No credit check	Tier 1 (T1)  IOC (Initial Operating Capacity) 10/01/2014  FOC (Full Operating Capacity)  09/30/2017
<b>Moderate Risk Public Trust Positions</b> <b>(No national security sensitivity)</b>	SF 85P  (Questionnaire for Public Trust Positions)	Moderate Risk Background Investigation (MBI)	Tier 2 (T2)  IOC 10/01/2014  FOC 09/30/2017
<b>High-Risk Public Trust Position</b> <b>(No national security sensitivity)</b>	SF 85P	Background Investigation (BI)	Tier 4 (T4)  IOC 10/01/2016  FOC 09/30/2017
<b>Secret/Confidential Clearance Eligibility</b> <b>(Military/Contractor)</b>	SF 86  (Questionnaire for National Security Positions)	National Agency Check with Law and Credit (NACLC)	Tier 3 (T3)  IOC 10/01/2015  FOC 09/30/2017
<b>Noncritical Sensitive Position and/or Secret/Confidential Clearance Eligibility</b> <b>(For Civilians)</b>	SF 86	Access National Agency Check with Inquiries (ANACI)	Tier 3 (T3)  IOC 10/01/2015  FOC 09/30/2017
<b>Critical Sensitive Position and/or Top Secret (TS) Clearance Eligibility</b>  <b>Special Sensitive Position and/or Top Secret Clearance Eligibility with Sensitive Compartmented Information (SCI)</b>	SF 86	Single Scope Background Investigation (SSBI)	Tier 5 (T5)  IOC 10/01/2016  FOC 09/30/2017
<b>Moderate Risk Public Trust Position Reinvestigation</b> <b>(No national security sensitivity)</b>	SF 85P	N/A	Tier 2 Reinvestigation (T2R)  IOC 10/01/2014  FOC 09/30/2017
<b>High-Risk Public Trust Position</b> <b>(No national security sensitivity)</b>	SF85P	N/A	Tier 4 Reinvestigation (T4R)  IOC 10/01/2016  FOC 09/30/2017
<b>Noncritical Sensitive Position and/or Secret/Confidential Clearance Eligibility periodic reinvestigation (PR)</b>	SF 86	NACLC	Tier 3 Reinvestigation (T3R)  IOC 10/01/2015*  FOC 09/30/2017  *(five year reinvestigation

For this Position Designation and Risk/Sensitivity Level:	Use This Standard Form:	Prior Investigations:	Revised Investigations and Implementation Dates:
			not required until FOC)
<b>Critical-Sensitive Position and/or Top Secret (TS) Security Clearance Special-Sensitive Position and/or Top Secret Clearance Eligibility with SCI periodic reinvestigation</b>	SF 86	SSBI-PR or Phased PR	Tier 5 Reinvestigation (T5R) IOC 10/01/2016 FOC 09/30/2017

Legend: R = Reinvestigation, T = Tier

## Appendix B (References and Definitions)

### 1. REFERENCES

- a. VA Directive 0710, Personnel Security and Suitability Program  
[http://www1.va.gov/vapubs/viewPublication.asp?Pub\\_ID=487&FTYPE=2](http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=487&FTYPE=2)
- b. Parts 302, 315, 332, 359, 731, 732, and 752 of Title 5, Code of Federal Regulations (CFR)  
[http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title05/5tab\\_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title05/5tab_02.tpl)
- c. EO 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified information." June 30, 2008  
<https://www.gpo.gov/>
- d. EO 13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust," January 16, 2009  
<https://www.gpo.gov/>
- e. EO 10450, "Security Requirements for Federal Employment", April 27, 1953, as amended  
<http://www.archives.gov/federal-register/codification/executive-order/10450.html>
- f. EO 12968, "Access to Classified Information" August 4, 1995, as amended  
<https://www.gpo.gov/>
- g. EO 13526, "Classified National Security Information," December 29, 2009  
<https://www.gpo.gov/>
- h. Parts 2001 and 2003, 32 CFR, Classified National Security Information (Implementing Directive for EO 13526).  
<http://www.archives.gov/>
- i. Office of Personnel Management, Federal Investigative Service, "Suitability Processing Handbook," September 2008
- j. Office of Personnel Management Memorandum for Heads of Departments and Agencies, Chief Human Capital Officers, and Agency Security Officers, "Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide," dated January 14, 2008  
<https://www.opm.gov/>
- k. Office of Personnel Management Memorandum for Heads of Departments and Agencies, Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12," dated July 31, 2008.  
[http://www.opm.gov/investigate/resources/decision\\_making\\_guide.pdf](http://www.opm.gov/investigate/resources/decision_making_guide.pdf)

- l. VA Directive and Handbook 5021, Employee/Management Relations  
<http://vaww1.va.gov/ohrm/Directives-Handbooks/Documents/5021.doc>
- m. 32 CFR 147, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.  
<http://www.gpo.gov/fdsys/pkg/CFR-2011-title32-vol1/pdf/CFR-2011-title32-vol1-part147.pdf>
- n. Office of Personnel Management Position Designation System and Automated Tool (PDT)  
<http://www.opm.gov>
- o. Revised Federal Investigative Standards, revised December 2012

## 2. DEFINITIONS:

**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.

**Appointee:** A person who has entered on duty and is in the first year of a subject-to-investigation appointment.

**Affiliates:** Individuals who are not an employed (being paid) by VA, i.e., Health Professions Trainees, Veteran Service Organization Officers, Volunteers.

**BI:** An investigation conducted for Tier 4/High Risk public trust positions.

**Covered positions:** 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 (SES).

**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.

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

**Fitness:** The reference to a person's level of character and conduct determined necessary for an individual to perform work for, or on behalf of, a Federal agency as an employee in the excepted service (other than in a position subject to suitability) or as a contractor employee.

**National Security Positions:** As defined in Part 732 of 5 CFR.

**Position Designation System and Automated Tool:** an automated tool provided by the OPM to assist 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.

**PIV Credential:** Personal Identity Verification cards as defined by HSPD-12, and VA Directive 0735, Homeland Security Presidential Directive-12 Program. PIV credentials include PIV cards which require at a minimum a SAC and a NACI; Non-PIV cards which require a SAC but no other background investigation, and; Flash Badges which do not require a SAC or a higher level background investigation.

**Reciprocity:** Recognition of favorable fitness or suitability determinations when the determination was based on criteria equivalent to standards established by OPM.

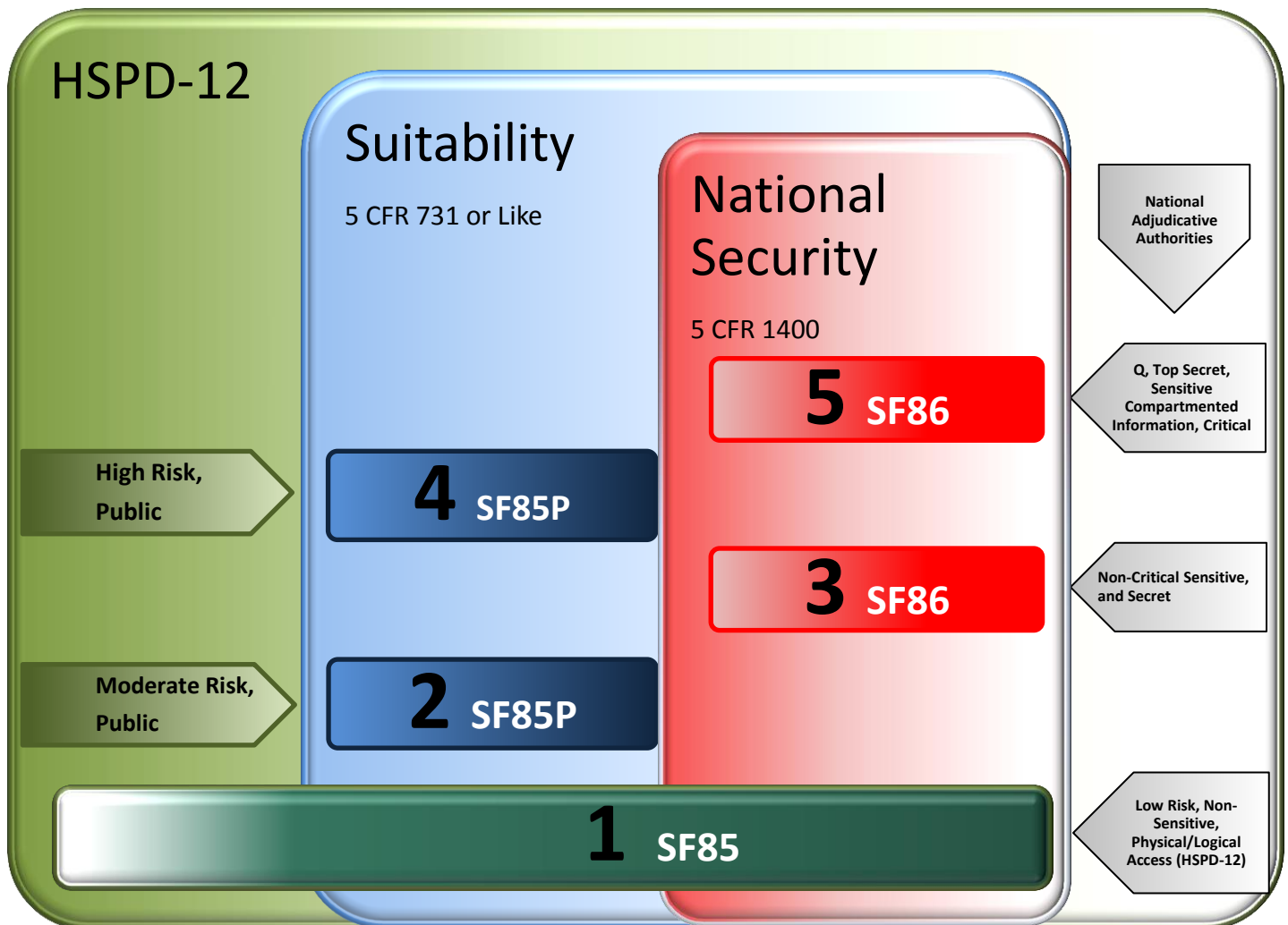
**Suitability:** Refers to a person's identifiable character traits and/or conduct that may have an impact on the integrity or efficiency of the service.

**Suitability Action:** Actions taken that affect covered applicants and appointees. The actions taken include cancellation of eligibility for employment, removal, cancellation of reinstatement eligibility, or debarment.

**Suitability Determination:** A decision that a person is suitable or is not suitable for employment in a covered position within VA.

APPENDIX C. FIVE-TIERED INVESTIGATIVE MODEL

**2012 Federal Investigative Standards  
Five-Tiered Investigative Model**





#### APPENDIX D: ACRONYMS

Acronym	Meaning
AS/HR&A	Assistant Secretary for Human Resources and Administration
AS/OI&T	Assistant Secretary for Information and Technology
CCT	Case Closing Transmittal
CFR	Code of Federal Regulations
CNACI	Childcare National Agency Check with Inquiries
COE	Certificate of Eligibility
COI	Certificate of Investigation
COR	Program Manager/Contracting Officer/Contracting Officer Representative (in this guidebook)
DSS	Defense Security Service
e-OPF	Electronic Official Personnel Folder
e-QIP	Electronic Questionnaires for Investigations Processing
EO	Executive Order
EOD	Entrance on Duty
FBI	Federal Bureau of Investigations
FIN	Federal Investigation Notice
FIPS	Federal Information Processing Standards
HSPD-12	Homeland Security Presidential Directive-12
INV 79A	Report of Agency Adjudicative Action
ISO	Information Security Officer
MSPB	Merit Systems Protection Board
NACI	National Agency Check with Inquiries (Tier 1)
ODNI	Office of the Director of National Intelligence
OF	Optional Form
OIG	Office of the Inspector General
OPM	Office of Personnel Management
OSP	Office of Operations, Security, and Preparedness
PAID	Personnel and Accounting Integrated Data
PAL	Proposed Action Letter
PD	Position Description
PDR	Position Designation Record
PDT	Position Designation Automated Tool
PII	Personally Identifiable Information
PIPS	Personnel Investigations Processing System

<b>Acronym</b>	<b>Meaning</b>
PIV	Personnel Identity Verification
PSIM	Office of Personnel Security and Identity Management
PSS	Personnel Security and Suitability Service
ROI	Report of Investigation
SAB	Security Appeals Board
SAC	Special Agreement Checks
SAP	Special Access Programs
SCHR	State Criminal History Repositories
SCI	Sensitive Compartmented Information
SES	Senior Executive Service
SHRO	Servicing Human Resources Offices
SIC	Security Investigation Center
SOW	Statement of Work
SSO	Special Security Officer
USC	United States Code
VA	Department of Veterans Affairs
VACO	VA Central Office