

## PERSONNEL SECURITY AND SUITABILITY PROGRAM

- 1. REASON FOR ISSUE:** To revise Department of Veterans Affairs (VA) policy regarding the Personnel Security and Suitability Program.
- 2. SUMMARY OF CONTENTS/MAJOR CHANGES:** This Directive updates the management, administration, and implementation of the VA Personnel Security and Suitability Program. The major changes are: 1) Mandating use of the Position Risk Designation and Automated Tool to replace the current process for position risk designation, 2) Mandating the use of the Office of Personnel Management's Electronic-Questionnaire for Investigations Processing (E-QIP) for all investigative types, 3) Requiring reciprocity when applicable, and 4) Incorporating the changes to 5 CFR 731, Suitability. This directive is applicable to applicants, appointees, employees, contractors, volunteers and affiliates.
- 3. RESPONSIBLE OFFICES:** Office of Operations, Security, and Preparedness, Office of Emergency Management is responsible for the contents of this directive.
- 4. RELATED HANDBOOK:** VA Handbook 0710, Personnel Security and Suitability Program.
- 5. RESCISSIONS:** VA Directive 0710, Personnel Suitability and Security Program, dated September 10, 2004.

**CERTIFIED BY:**

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

/s/  
Roger W. Baker  
Assistant Secretary for  
Information Technology

/s/  
Jose D. Riojas  
Assistant Secretary for  
Operations, Security, and Preparedness

Distribution: Electronic Only



## PERSONNEL SECURITY AND SUITABILITY PROGRAM

**1. PURPOSE AND BACKGROUND.** This directive describes the purpose, responsibilities, requirements, and procedures of VA's Personnel Security and Suitability Program, applicable to Federal applicants, appointees, employees, contractors and affiliates who have access to departmental operations, facilities, information, or information technology systems.

a. The Personnel Security and Suitability Program has three main purposes:

(1) To provide a basis for determining a person's suitability to work for or on behalf of the government,

(2) To provide a basis for VA to determine whether a Federal employee should be granted a security clearance, and

(3) To implement certain Personal Identity Verification requirements of Federal Information Processing Standards (FIPS-201).

b. The Federal government mandates by law, executive order, Presidential Directives, regulations, and guidance that all applicants, appointees, employees, contractors, and others are suitable for employment or assignment to work for or on behalf of the Federal government.

c. Personnel Security and Suitability Programs were established in 1953 by Executive Order (EO) 10450, Security Requirements for Government Employment, as amended and enhanced in 1995 by EO 12968, Access to Classified Information, as amended. These orders set the standards for suitability and security clearance processes for the Federal government. The processes were reformed in 2008 by EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information.

d. EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, was issued June 30, 2008. This EO reformed the use of reciprocity across the Federal government to ensure cost-effective, timely, and efficient protection of national interests.

e. Office of Personnel Management (OPM) revised Title 5, Code of Federal Regulations (CFR), 731, Suitability in April 2008 and again in November 2008. These regulations are the framework for the Department of Veterans Affairs (VA's) Personnel Security and Suitability Program.

f. EO 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, was issued on January 16, 2009. This EO requires a reinvestigation on all individuals in positions of public trust to ensure that they remain suitable for continued employment.

g. The Intelligence Reform and Terrorism Prevention Action of 2004 (IRTPA), Public Law No. 108-458 (2004) (codified at 50 U.S.C. 435b) sets goals and timelines for granting clearances, ensuring reciprocity, and establishing an integrated database for completed background investigations.

## 2. POLICY

a. VA is required to establish criteria and procedures for making suitability determinations and taking suitability actions involving applicants for and appointees to covered positions. Suitability determinations are based on a person's character or conduct that may have an impact on the integrity or efficiency of the service. Determining suitability for Federal employment will be consistent with 5 Part CFR 731. Determining fitness for contractor employees will be based on criteria equivalent to that used for Federal employees. Determinations made under this category are distinct from determinations of eligibility for assignment to, or retention in, sensitive national security positions.

b. Some positions are also subject to sensitivity considerations relating to national security and access to classified information. Eligibility for access to classified information shall be granted in accordance with EO 12968, as amended. Eligibility determinations will be made using the standards set forth in the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information."

c. VA must implement policies and maintain records demonstrating that VA employs reasonable methods to ensure adherence to Office of Personnel Management (OPM) and other regulatory issuances in determining suitability for employment. Facilities are required to establish local policies and procedures to ensure that required background screenings are accomplished and documented.

d. This directive requires Administrations and staff offices to collaborate, participate, and recognize the shared, related, and interdependent responsibility to provide effective and efficient personnel security services to the department.

### **e. Designating Position Risk and Sensitivity Levels**

(1) Agencies are required by 5 CFR, 731, Suitability, to designate the position risk level for all covered positions at Low, Moderate or High as determined by the position's potential to adversely impact the efficiency and integrity of the service. High and Moderate Risk level positions are designated as Public Trust positions.

(2) All positions must also be given a sensitivity designation. National security positions are those that involve activities that are concerned with the protection of the United States from foreign aggression or espionage, the preservation of the Nation's military strength, and the regular use of, or access to, classified information. The sensitivity designations are Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive. This designation is complimentary to the risk designation, and may have an effect on the position's investigative requirement.

(3) All VA administrations and staff offices must use the Position Designation System and Automated Tool (PDAT) for designating position risk and sensitivity levels for all positions. The position designation process is used to determine the appropriate level of investigation for positions covered by 5 CFR, parts 731, Suitability, and 732, National Security Positions.

(4) The PDAT will be used by Contracting Officers and Contracting Officer Technical Representative to appropriately designate the statement of work or other written description of the

assignment, with the proper risk or sensitivity level for the contract employees. Information Security Officers (ISO) should be consulted when access to VA information systems and data is involved to ensure appropriate risk levels are assigned for contractors.

f. **Electronic Questionnaire for Investigations Processing (E-QIP).** The use of E-QIP is mandated by the Office of Management and Budget (OMB) and OPM pursuant to the E-Government Act of 2002, P.L. 107-347. E-QIP allows applicants to electronically enter, update, and transmit their personal investigative data over a secure Internet connection to their employing agency for review and approval. E-QIP must be used for all investigative types for employees, contractors, affiliates, volunteers and other designated individuals who will need a background investigation.

g. **Personal Identity Verification (PIV).** FIPS 201-1 requires that at a minimum National Agency Check with Inquiries (NACI) be initiated prior to the issuance of a Personal Identity Verification (PIV) compliant card. Agencies can issue an electronically distinguishable identity credential on the basis of a completed FBI National Criminal History Check (fingerprint check) while the NACI is pending. OPM conducts Special Agreement Checks (SAC) which cover FBI criminal history. VA facilities must use electronic fingerprint equipment to submit SAC requests to OPM. All individuals who work for or at VA, whether they are paid or unpaid, with access to VA information or information systems, will be subject to background investigations pursuant to VA Directive 0735, "Personal Identity Verification (PIV) of Federal Employees and Contractors."

#### h. **Exemptions**

(1) OPM has by regulation exempted the following positions from the investigative requirements of Executive Order (EO) 10450, Security Requirements for Government Employment, as amended.

(a) Low Risk/Nonsensitive positions that are temporary, intermittent, per diem, or seasonal not to exceed an aggregate of 180 days in either a single continuous appointment or series of appointments; and

(b) Positions filled by aliens outside the United States.

(2) Administrations and staff offices must conduct such checks as appropriate to ensure that the employment or retention of such individuals in these positions is consistent with the interests of national security.

(3) In accordance with National Institute of Standards and Technology (NIST) guidance, background screenings commensurate with the risk involved with the position will be conducted for any positions that require access to VA information systems.

(4) All individuals who work at or for VA, whether they are paid or unpaid, with access to VA information systems, will be subject to background screenings prior to being granted such access.

(5) By agreement with OPM, the investigative requirements as set forth in EO 10450 will not apply to the following categories of employees:

(a) Consultants or experts appointed to Low Risk/Nonsensitive positions for a period 1 year or less and not to be reappointed; and experts or consultants appointed for a period of more than 1 year or reappointed after a year with no break in service, provided the service does not exceed more than 30 days in any one calendar year.

(b) Physicians appointed under 38 U.S.C. 7406 to Low Risk/Nonsensitive positions as medical residents, provided they do not exceed 1 year of continuous service at a VA facility, regardless of the duration of the residency program.

(c) Purchase and hire employees appointed to Low Risk/Nonsensitive positions appointed for six months or less.

(6) Contract personnel assigned to Low Risk/Nonsensitive positions for 180 days or less under a single contract or a series of contracts.

(7) Any additional exemptions to the investigative requirements of EO 10450 must be approved by OPM, upon the request of the Secretary. Administrations and staff offices may submit requests for additional exemptions or modifications of existing exemptions through the Office of the Operations, Security, and Preparedness (OSP) for approval and submission to OPM.

i. **Background Screening.** VA requires that all personnel be subject to an appropriate background screening (Special Agreement Check (SAC)) prior to permitting access to VA information and information systems. This includes applicants, appointees, employees, contractors, affiliates and other individuals who require physical and/or logical access to VA information or information systems to perform their jobs.

j. **Reciprocity.** Background investigations and adjudications shall be mutually and reciprocally accepted. VA may not establish additional investigative or adjudicative requirements that exceed the requirements for suitability, contractor employee fitness, eligibility for logical or physical access, eligibility to hold a sensitive position, or eligibility for access to classified information without the approval of the Suitability Executive Agent or Security Executive Agent, as appropriate, and provided that approval to establish additional requirements shall be limited to circumstances where additional requirements are necessary to address significant needs unique to the agency involved or to protect national security.

(1) If there is a current investigation that meets or exceeds the requirements for the position, a new investigation will not be conducted provided the person has been serving continuously for at least 1 year in a position subject to investigation, there has not been a break in service greater than 2 years, and there is no new information obtained during the hiring process that that calls into question the person's suitability under 5 CFR 731.202.

(2) If the subject was determined suitable under 5 CFR 731, or fit based on criteria equivalent to the suitability factors of 5 CFR 731, and has a break in service of not more than two years, the prior suitability determination will be accepted.

k. **Exceptions to Reciprocity.** A gaining agency is not required to grant reciprocal recognition to a prior favorable fitness or suitability determination when: the new position requires a higher level of

investigation than previously conducted for that individual; an agency obtains new information that calls into question the individual's fitness based on character or conduct; or the individual's investigative record shows conduct that is incompatible with the core duties of the new position.

**l. Title 38 Provisions.** This directive extends the provisions of 5 CFR Part 731 and 5 CFR 732 to VA's Title 5 excepted service, Title 5/Title 38 hybrid excepted service, and employees appointed under Title 38, United States Code (U.S.C.) Chapters 3 (except the Under Secretary for Health), 71, or 78; and extends the criteria of 5 CFR Part 731 to the Under Secretary for Health and employees appointed under Title 38 U.S.C. Chapters 73 and 74.

**m. Costs.** Cost of Background Investigations will be borne by the organization requesting the investigation. For contractors and its personnel performing the contract, the VA office or organization that is requesting the procurement will coordinate with the designated contracting officer to ensure VA initiates the necessary investigations and/or screenings for contractor personnel. For those contractors and its personnel, the contractor will bear the cost of such investigations.

**n. Classified Documents will be properly handled and safeguarded.** Each individual who has access to classified national security documents is responsible for the protection of those documents and must be familiar with and adhere to the provisions of:

- (1) EO 12958, Classified National Security Information, as amended;
- (2) EO 12968, Access to Classified Information;
- (3) Information Security Oversight Office guidelines;
- (4) 32 CFR Part 2001, Classified National Security Information;
- (5) Director, National Intelligence Guidelines;
- (6) Director, Central Intelligence Agency Guidelines.

### 3. RESPONSIBILITIES

**a. Secretary of Veterans Affairs.** Has overall responsibility for VA's Personnel Security and Suitability Program. The Office of Operations, Security, and Preparedness is delegated the responsibility to implement and manage the program.

**b. Assistant Secretary for Operations, Security, and Preparedness (AS/OSP).** The AS/OSP has the authority to establish and maintain personnel security and suitability programs throughout the Department consistent with applicable laws, rules, regulations, and Executive Orders. The Office of Emergency Management is given delegated authority for the following:

- (1) Providing broad departmental-wide policy direction, standards setting, coordination, and performance assessment for organizational components within VA and develop policies, procedures, and practices relating to background investigations of employees and contractors and the determinations of risk and sensitivity levels of employee position descriptions.

(2) Managing, directing, and leading VA's Security and Investigation Center (SIC) to ensure adjudicative determinations are made in the best interest of the government. Managing the national security clearance program to ensure access to classified information will be limited to those persons whose official duties require knowledge or possession of the information.

(3) Implementing appropriate laws, rules, and regulations related to the personnel security and suitability program and taking actions to address and correct conditions that are non-compliant with applicable laws, rules, and regulations as well as exercises policy oversight of Administrations and staff offices personnel security programs.

(4) Evaluating the implementation and effectiveness of VA-wide personnel security and suitability practices and procedures, including the adjudicative determinations for both public trust/suitability and national security cases (also include national agency check with inquiries).

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

(6) Establishing departmental standards for: a) background investigations; b) uniform guidelines for adjudication; c) determining suitability for employment; d) access to classified information and sensitive but unclassified information; e) and maintaining a central index of department-granted security clearances.

(7) Representing VA's interests on interagency forums and meetings with personnel security concerns, to share best practices, and to actively promote the personnel security and suitability program within the Federal government. This includes serving as the principal contact with the OPM for VA and with other Federal agencies and entities on personnel security and suitability matters.

**c. 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 Security Program, commensurate with the Federal Information Security Management Act (FISMA), to protect information resources and to provide security measure 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.

**d. 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 low risk positions. The OIG will determine which OIG positions are national security positions and coordinate with the Security Investigations Center for initiation and adjudication.

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



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

- (1) Comply with the policies set forth in this directive and the procedures set forth in VA Handbook 0710, Personnel Security and Suitability Program.
- (2) Ensure the appointment of individuals and their continued employment is consistent with the position's suitability or national security considerations.

**g. Human Resources Management Offices will:**

- (1) Ensure all positions are designated with the appropriate risk or sensitivity level in accordance with the PDAT and ensure that each appointee and employee receives a background investigation commensurate with the position risk or sensitivity level.
- (2) Ensure position risk and sensitivity level designations are periodically reviewed by appropriate officials to ensure that designations are up-to-date and consistently applied to all positions in accordance with 5 CFR Part 731, Suitability, and 5 CFR Part 732, National Security Positions; and the VA information security program.
- (3) When appropriate, refer appointees and employees in Public Trust and National Security positions to the SIC for initiation and adjudication of the investigation.
- (4) Ensure appointees and employees in Low Risk/Nonsensitive positions have background investigations initiated and adjudicated at the local level within established timeframes. Adjudicative determinations must be made by appropriately trained personnel and reported to OPM.
- (5) Ensure a fingerprint Special Agreement Check (SAC) is conducted on all new appointees who are exempt from the requirement to have a NACI or higher level investigation. Whenever possible, the SAC should be performed prior to the appointee's entrance on duty. When this is not possible, the SAC must be performed as part of the in-processing. Ensure the SAC is adjudicated by appropriately trained personnel no later than 5 workdays after the results are received.

**h. Program or Project Managers will:**

- (1) Ensure appropriate language is included in applicable contracts so that the Statement of Work (SOW) accurately reflects 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 PDAT and given the appropriate designation.
- (2) Ensure all contractor employees who are not exempt from the investigative requirement are referred to the SIC for initiation and adjudication of the appropriate level of investigation.
- (3) Ensure a SAC is initiated on all new contractor employees who are exempt from investigative requirement and who provide direct and/or ancillary health care services at VA facilities or have access to VA information systems or sensitive information.

(4) Ensure the SAC is adjudicated by appropriately trained personnel no later than 5 workdays after the results are received.

i. **Contracting Officers will** ensure appropriate personnel security contract clauses are included in the contracts.

j. **Facility Voluntary Service Officer will:**

(1) Ensure a SAC is initiated prior to entry on duty for all new volunteers who have:

- (a) Assignments associated with home health care;
- (b) Assignments involving the provisions of patient care or working alone with patients;
- (c) Assignments involving contact with pharmaceuticals or other biological agents;
- (d) Assignments that provide access to patient records;
- (e) Assignments involving clinical research;
- (f) Assignments that provide access to any VA computer system;
- (g) Access to any sensitive or Privacy Act protected information not identified above.

(2) Ensure the SAC is adjudicated by appropriately trained personnel no later than 5 workdays after the results are received.

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

#### 4. AUTHORITIES AND REFERENCES

a. Executive Orders (EO) 10450, "Security Requirements for Government Employment, as amended."

b. EO 10577, "Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service, as amended."

c. EO 12968, "Access to Classified Information, as amended."

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

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

f. Federal Information Processing Standards Publication (FIPS) 201, "Personal identity Verification (PIV) of Federal Employees and Contractors" as amended by FIPS 201-1.

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

h. Public Law 107-347, "E-Government Act of 2002." to include Title 3, the Federal Information Security Management Act (FISMA).

i. The Intelligence Reform and Terrorism Prevention Action of 2004 (IRTPA), Public Law 108-458 (December 17, 2004) (codified at 50 U.S.C. 435b).

j. VA Directive 0735, "Personal Identity Verification (PIV) of Federal Employees and Contractors." (to be issued)

k. VA Directive and Handbook 6500, "Information Security Program."

l. 5 Code of Federal Regulations (CFR) 731, "Suitability."

m. 5 CFR 732, "National Security Positions."

n. 5 CFR 736, "Personnel Investigations."

o. 15 CFR Part 4a, "Classification, Declassification, and Public Availability of National Security Information."

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

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

r. 32 CFR Part 400, "National Industrial Security Program Directive No. 1."

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

t. 50 U.S.C. § 435, "Procedures governing access to classified information."

## 5. DEFINITIONS

a. **Access.** The ability and opportunity to obtain knowledge of classified national security information or sensitive information

b. **Affiliate.** A non-Federal employee or contract individual that requires logical access to VA information systems and/or physical access to VA facilities to perform their jobs. Examples of affiliates include students, researchers, residents, Veteran Service Organization volunteers, union officials, temporary help, and interns.

c. **Applicant.** A person who is being considered or has been considered for employment.

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

e. **Background Investigation (BI)** A type of investigation that covers a five-year period and is used for High Risk positions.

f. **Background Screening.** Any type of procedure used to verify the accuracy of an individual's identification, credentials, and employment history. Screenings may consist of fingerprint checks for criminal history records, validation of resume and/or educational references, and checks of various databases for appropriate preliminary checks.

g. **Basic Suitability Evaluation.** An evaluation of character or conduct that may have an impact on a person's suitability for any Federal position.

h. **Covered Position.** 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.

i. **Classified National Security Information.** Information requiring protection against unauthorized disclosure (marked confidential, secret, or top secret when in documentary form, to indicate its classified status), pursuant to Executive Orders 12958 and 12968.

j. **Confidential.** Information of which unauthorized disclosure could reasonably be expected to cause damage to the national security

k. **Critical-Sensitive.** A position sensitivity designation indicating a potential for exceptional or grave damage to the national security. These positions involve access to top secret classified information.

l. **Employee.** A person who has completed the first year of a subject to investigation appointment

m. **Information Security Officer.** The individual responsible for the management and oversight of an organization's information security program, including the development of IT system security

plans that identify, evaluate, and minimize risks associated with IT system vulnerabilities; and for ensuring the security of systems and data against unauthorized or inappropriate use.

n. **Limited Background Investigation (LBI).** An investigation that consists of a NAC, subject interview, personal interviews with selected sources covering specific areas of a subject's background during the past one to three years, and written inquiries, record searches, and a credit check for the past five to seven years. This investigation is used for moderate risk positions that require access to secret information (non-critical sensitive).

o. **Low Risk.** A final position designation assessment reflecting the potential for limited impact on the agency program or mission or the integrity and efficiency of the service.

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

q. **Minimum Background Investigation (MBI).** An investigation An investigation that consists of a subject interview, credit history, and all the components of a NACI covering the most recent five-year period for law enforcement checks and seven years for credit checks. This investigation is used for moderate risk positions.

r. **Moderate Risk.** A final position designation assessment reflecting the potential for limited impact on the agency program or mission or the integrity and efficiency of the service

s. **National Agency Check (NAC).** An investigation consisting of a search of records of the Office of Personnel Management Security and Suitability Index (SII), an FBI name check and criminal history fingerprint check, the Department of Defense Clearance & Investigations Index (DCII) and other record searches covering specific areas of an individual's background.

t. **National Agency Check with Written Inquiries (NACI).** An investigation that includes a NAC plus written inquiries to references, employers, places of education and residence, and other record sources covering specific areas of an individual's background during the past five years.

u. **Need for Access.** Determination that an employee requires access to a particular level of sensitive or classified information in order to perform or assist in a lawful and authorized governmental function.

v. **Noncritical Sensitive.** A position sensitivity designation indicating a potential for significant or serious damage to the national security. These positions involve access to secret or confidential classified information.

w. **Nonsensitive.** A position that does not require access to sensitive or classified information.

x. **Public Trust.** The category of position, at the moderate or high risk levels involving a significant degree of public trust.

y. **Secret.** Information, the unauthorized disclosure of which, could reasonably be expected to cause serious damage to the national security.

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

aa. **Sensitivity Designation.** A position assessment indicating the degree of damage an individual in the position could effect to the national security.

bb. **Single Scope Background Investigation (SSBI).** An investigation consisting of a NAC, subject interview, written inquiries, record searches, credit check, personal interview with selected sources covering employment , residence, and law enforcement agencies during the most recent ten year period. A credit check will be made on the past seven years. This investigation is used for access to top secret information (critical sensitive and special sensitive).

cc. **Special Sensitive.** A position sensitivity designation that includes any position, which the Secretary determines to be in a level higher than critical sensitive. These positions involve access to intelligence related information.

dd. **Suitability.** A person's identifiable character traits and conduct sufficient to decide whether an individual's employment or continued employment would or would not protect the integrity or promote the efficiency of the service

ee. **Suitability Action.** An action described in 5 CFR 731.203 (cancellation of eligibility, removal, cancellation of reinstatement eligibility, debarment) that may be taken by OPM or an agency with delegated authority under the procedures in 5 CFR 731 subparts C and D.

ff. **Suitability Determination.** A decision by OPM or an agency with delegated authority that a person is suitable or is not suitable for employment in covered positions in the Federal government or a specific Federal agency.

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