Department of Veterans Affairs
Washington, DC 20420

VA Directive 0710
Transmittal Sheet
September 10, 2004

PERSONNEL SUITABILITY AND SECURITY PROGRAM

1. REASON FOR ISSUE: This Directive updates Department of Veterans Affairs (VA) policy for the management of the personnel suitability and security program in accordance with 5 Code of Federal Regulations (CFR) Part 731, Suitability, and 5 CFR Part 732, National Security Positions, that includes the management and appropriate handling of classified national security documents within VA.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Directive sets forth Department policy for the designation of appropriate risk levels or sensitivity levels and the commensurate scope of background investigations required for all VA positions. The directive delegates responsibility for designating position risk levels or sensitivity levels to Under Secretaries, Assistant Secretaries, Other Key Officials; Deputy Assistant Secretaries, and field facility directors; and it assigns that the cost of background investigations be borne by each organization requesting them. It extends the provisions of 5 CFR Parts 731 and 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 Parts 731 and 732 to the Under Secretary for Health and employees appointed under Title 38 U.S.C. Chapters 73 and 74. Additionally, it provides guidance for contractor personnel and sets forth policy for the management and secure handling of classified national security documents.

3. RESPONSIBLE OFFICE: Office of the Deputy Assistant Secretary for Security and Law Enforcement, Security and Investigations Center.

4. RELATED HANDBOOK: VA Handbook 0710, Personnel Suitability and Security Program.

5. RESCISSIONS: VA Directive and Handbook 0710, Personnel and National Information Security, October 30, 2000.

CERTIFIED BY:

/s/
Robert N. McFarland
Assistant Secretary
for Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Dennis M. Duffy
Acting Assistant Secretary
for Policy, Planning, and Preparedness

Distribution: Electronic Only

PERSONNEL SUITABILITY AND SECURITY PROGRAM

1. PURPOSE. This Directive provides Department policy pertaining to VA applicants, appointees, employees, and contract personnel for:

a. Identification of a position's risk level as it relates to the efficiency and integrity of the Federal service; and identification of a position's sensitivity level as it relates to a position with national security interests.

b. Determining the scope of a personnel background investigation as it relates to each risk level or sensitivity level; and the distinction between an individual's suitability for Federal service employment and eligibility for Federal service employment in a sensitive position with national security interests.

c. The secure handling, transmitting, and storing of classified documents.

2. POLICY. Background investigations are conducted commensurate with a position's risk or sensitivity level. Department positions are subject to suitability considerations relating to the efficiency and integrity of the service, see 5 CFR Part 731, and to the security and protection of VA information as outlined in the Federal Information Security Management Act (FISMA). In addition, some Department positions are also subject to sensitivity considerations relating to national security and the access and use of classified national security information. See 5 CFR Part 732. Where positions are subject to both suitability and national security considerations, the higher level background investigation must be completed. See VA Handbook 0710, Appendix A. Contractors are discussed in VA Handbook 0710 and generally handled as employees.

a. **Designating Suitability Risk Levels**

(1) Agencies are required by 5 CFR Part 731, Suitability, to designate every competitive service and Senior Executive Service position within the agency at a High, Moderate, or Low Risk level as determined by the position's potential to adversely impact the efficiency and integrity of the Federal service. The High and Moderate Risk level positions are normally designated as Public Trust positions. These positions may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust, see 5 CFR §731.106(b). The risk level may also be known as a position's suitability designation or suitability risk level.

(2) This directive extends the provisions of 5 CFR Part 731 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.

b. **Designating National Security Sensitivity Levels**

(1) Agencies are required by 5 CFR Part 732, National Security Positions, to determine as national security positions 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. In determining national security positions, agencies will designate appropriate positions as Special Sensitive, Critical Sensitive, Noncritical Sensitive, see 5 CFR §732.201(a). The misconduct of occupants of these positions has the potential to adversely impact national security interests. Positions that do not have these sensitivities are designated as Nonsensitive. The sensitivity level is also known as a position's sensitivity designation or national security sensitivity level.

(2) This directive extends the provisions of 5 CFR Part 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 732 to the Under Secretary for Health and employees appointed under Title 38 U.S.C. Chapters 73 and 74.

c. **Exemptions**

(1) The Office of Personnel Management (OPM) has by regulation exempted the following positions from the investigative requirements of Executive Order (EO) 10450, Security Requirements for Government Employment, as amended. However, 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. Also, 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. See paragraph 5f of this directive for the definition of a background screening. In accordance with NIST guidance, 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.

(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) 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 one year or less and not to be reappointed; and experts or consultants appointed for a period of more than one 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 one 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.

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

(4) Any additional exemptions to the investigative requirements of EO 10450 must be approved by OPM, upon the request of the Secretary. See 5 C.F.R. §732.202(b)(2). Administrations and staff offices may submit requests for additional exemptions or modifications of existing exemptions through the Office of the Security and Law Enforcement to the Secretary for approval and submission to OPM.

(5) Exemptions in this paragraph do not exempt VA employees or contract personnel from any investigative requirements established pursuant to paragraphs 2d and 3c of this directive. In accordance with NIST guidance, 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. The type of screening required will be determined by each Administration and staff office, dependent upon the risk involved.

d. **Risk Assessments Required to Meet Information and Computer Security Legal Requirements**. All positions, including volunteers and contract personnel and the positions exempted under paragraph 2c of this directive, will be assessed by the appropriate Information Security Officer (ISO) for the possible risk or harm that could result from an incumbent's loss, misuse, or unauthorized access to or modification of VA information; including the potential for harm or embarrassment to an individual who is the subject of the records. If the ISO's review results in a higher level of background investigation for a position's risk or sensitivity designation than would otherwise be required by this directive and it's associated VA Handbook 0710, then the higher level investigation will be considered. Final determinations will be made by the program office with delegated authority to make final suitability and national security eligibility determinations.

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

(1) E.O. 12958, Classified National Security Information, as amended by E.O. 13292; Further Amendment to Executive Order 12958, as Amended, Classified National Security Information;

(2) E.O. 12968, Access to Classified Information;

(3) Information Security Oversight Office (ISOO) guidelines;

(4) VA Handbook 0710, Personnel Suitability and Security Program.

(5) 32 CFR Part 2001, Classified National Security Information;

(6) Information Security Oversight Office (ISOO) Guidelines;

f. **Cost of Background Investigations**. The cost of all background investigations will be borne by the organization requesting the investigation. The Security and Investigations Center will provide a report on a semi-annual basis to HRM offices. Discrepancies will be reported back to the Security and Investigations Center so that billing charges can be adjusted.

3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs** is responsible for VA's personnel suitability and security program. The Office of the Deputy Assistant Secretary (DAS) for Security and Law Enforcement is delegated the responsibility for implementing, managing, and overseeing this program.

b. **Assistant Secretary for Policy, Planning, and Preparedness** will ensure that the DAS for Security and Law Enforcement manages and implements the personnel suitability and security program in accordance with applicable Executive Orders, laws and regulations and that classified national security documents are properly handled and safeguarded.

c. **Assistant Secretary for Information and Technology** will ensure that the Office of Cyber and Information Security develops and implements a Departmentwide Information Security Program, commensurate with the 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.

d. **Deputy Assistant Secretary for Security and Law Enforcement** through the Security and Investigations Center will:

(1) Develop policy and guidance for personnel suitability and security, and for the handling and safeguarding of classified documents within VA.

(2) Implement appropriate laws, rules, and regulations related to the personnel suitability and security requirements.

(3) Ensure that each appointee or employee for a Public Trust (High and Moderate Risk) or national security position (Special Sensitive, Critical Sensitive, Noncritical

Sensitive) receives the appropriate background investigation commensurate with the position's designated risk or sensitivity level.

(a) The Security and Investigations Center makes final suitability determinations for appointees and employees in Public Trust (High and Moderate Risk) positions and security determinations for appointees and employees in national security (Critical Sensitive, Noncritical Sensitive) positions except for Office of Inspector General (OIG) appointees and employees.

(b) Final security adjudications for Special Sensitive positions are determined by the Central Intelligence Agency (CIA) as outlined in CIA Directorates "Minimum Personnel Security Standards and the Procedures Governing Eligibility for Access to Sensitive Compartmental Information," April 14, 1986; and "Security Manual for Uniform Protection of Intelligence Process in Automated Information Systems and Networks," July 19, 1988.

(c) Ensure that appropriate pre-appointment screening is done prior to approval of an interim security clearance for a national security position, pending completion of the appropriate background investigation.

(d) The Security and Investigations Center initiates and adjudicates background investigations for contract personnel in positions designated at the Low, Moderate, or High Risk levels.

(4) Initiate and adjudicate the periodic reinvestigations of personnel who occupy Critical Sensitive, High Risk, and select Moderate Risk positions to determine if the continued employment, clearance, or assignment is clearly consistent with interests of public trust or national security. Initiate the periodic reinvestigation process for Special Sensitive positions, with final security eligibility being determined by the CIA as noted in paragraph 3d(3)(b) of this directive.

(5) Suspend or revoke employee security eligibility to occupy positions designated as Special Sensitive, Critical Sensitive and/or positions that involve access to classified national security information when an employee’s positive drug test has been verified. See VA Directive 5383, VA Drug-Free Workplace Program.

(6) Maintain an automated database of employees who are granted or denied background clearances for suitability for Federal employment or security eligibility to occupy sensitive national security positions. These records are covered as a System of Records under the Privacy Act, “OPM/Central 9, Personnel Investigations Records”. The information maintained in this database may be made available to other VA staff on a need-to-know basis.

(7) Conduct investigations of all security violations involving national security classified documents within VA and provide reports of investigations to the appropriate official.

(8) Conduct inspections at VA facilities that maintain and handle classified documents to ensure compliance with pertinent Executive orders and Federal regulations.

(9) Process all waiver requests for applicants of national security positions.

e. **Deputy Assistant Secretary for Human Resources Management** will:

(1) Work with the Security and Investigations Center, the Administrations, and Staff Offices to assist in maintaining timely adjudication of suitability investigations.

(2) Develop and maintain a Human Resources Management Letter (HRML) to provide process guidance on suitability and adjudication.

(3) Provide guidance to field facilities on risk and sensitivity level designations.

f. **Office of Inspector General**. 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. Accordingly, the OIG makes the final suitability determinations for OIG appointees and employees. OIG will certify previous investigation and clearance history when applicable for all transferring appointees.

g. **Under Secretaries, Assistant Secretaries, Other Key Officials, and Directors of Field Facilities** will ensure that:

(1) Their respective organizations comply with the policies set forth in this directive and the procedures set forth in VA Handbook 0710, Personnel Suitability and Security Program.

(2) Appointment of individuals and their continued employment are consistent with the position’s suitability considerations or national security considerations;

(3) All positions are designated with the appropriate risk level or sensitivity level in accordance with VA Handbook 0710;

(4) Position risk level and sensitivity level designations are periodically reviewed by appropriate officials and each organization's ISO 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.

(5) Appropriate field facility or Central Office officials shall refer all contract personnel to the Security and Investigations Center for background investigation initiation and adjudication as outlined in VA Handbook 0710, paragraphs 5 and 7. However, positions described in paragraph 2c of this directive, will be exempted from this requirement.

(6) Individuals with responsibility for reviewing position risk and sensitivity level designations, and adjudicating suitability and making final determinations must complete formal training which includes government-wide and VA-specific requirements.

(7) If a background investigation has been completed and is still valid, the contractor must provide the current CAGE Code Department of Defense Registration number for certification to the VA official authorized to award the contract. In turn, this information must be submitted to the Security and Investigations Center for verification.

(8) The Under Secretary for Health will issue additional guidance related to background screenings and investigations for Veterans Health Administration employees and volunteers.

h. **Human Resources Management (HRM) Offices** will ensure that:

(1) Position risk levels or sensitivity levels are determined by authorized and trained officials, generally Human Resources Officials, and the Information Security Officer of each Administration or staff office.

(2) Appointees and employees in Public Trust (High and Moderate Risk) and national security (Special Sensitive, Critical Sensitive, Noncritical Sensitive) positions are referred to the Office of Security and Law Enforcement, Security and Investigations Center for the initiation and adjudication of the appropriate background investigation.

(3) Investigations for appointees and employees in Low Risk and Nonsensitive positions are initiated and receive the appropriate background investigation and adjudication.

(4) Applicants will be referred to the Security and Investigations Center for pre-appointment screening where there is a need for an interim security clearance for a national security position, pending completion of the appropriate background investigation.

(5) The background investigation process for individuals appointed to Low Risk/Nonsensitive positions, including those in OIG and unless exempted by this directive, is initiated within 14 days of appointment to the position.

(6) That an individual transferring into VA from the military or other Federal agency has a current clearance in place, the level of which is appropriate to the incumbent's position risk or sensitivity level designation. HRM will certify previous investigation and clearance history when applicable for all incoming transfer appointees from other Federal agencies or individuals recently leaving military service.

(7) Suitability adjudications for Low Risk/Nonsensitive positions must be returned to OPM via Office of Federal Investigations Forms 79A within 90 days of receipt of the investigative report from OPM.

i. **Directors, Field Facilities**. In addition to the responsibilities listed in paragraph 3f of this directive, directors of VHA field facilities will, in compliance with the USA Patriot Act of 2001, identify positions involved in the shipment, receipt, or possession of select agents defined in 42 CFR Section 72.6(j). Each position must have a designated sensitivity or risk level, and appropriate background investigations must be accomplished and adjudicated prior to the placement of appointees or employees in these positions. This may require establishment of temporary positions that do not require the above duties. In addition, a security risk assessment must be completed in accordance with the following law, 42 CFR section 73.8(d), 7 CFR §31.10(h), 9 CFR §121.11(h), and VHA Directive 2002-075. See Public Law 107-56, Section 817, 115 Stat. 385 (October 26, 2001).

4. AUTHORITIES AND REFERENCES

a. Director of Central Intelligence Directive (DCID) 6/4, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI).

b. E-Government Act of 2002, Pub. L. 107-347 (Dec. 17, 2002); to include Title 3, the Federal Information Security Management Act (FISMA).

c. Executive Order 10450, Security Requirements for Government Employment, as amended

d. Executive Order 10577, Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service, as amended, Part I, Rule VI, Section 6.3(b)

e. Executive Order 12958, Classified National Security Information, as amended by E.O. 13292

f. Executive Order 12968, Access to Classified Information

g. Federal Information Processing Standards Publication 199, Standards for the Security Categorization of Federal Information and Information Systems, February 2004

h. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems (draft), October 2003

i. VA Directive and Handbook 5005, Staffing

j. VA Directive and Handbook 5021, Employee/Management Relations

k. VA Directive 5383, VA Drug-Free Workplace Program

l. USA Patriot Act of 2001, Pub. L. 107-56

m. 5 CFR §6.3(b), Method of filing excepted positions and status of incumbents

n. 5 CFR §302.102(a), Method of filling positions and status of incumbents

o. 5 CFR Parts 731, 732, and 736, Suitability; National Security Positions; and Personnel Investigations, respectively

p. 32 CFR Part 2001, Classified National Security Information

q. 5 U.S.C. Section 552a, Privacy Act

r. 5 U.S.C. §3301, Civil service; generally

s. 5 U.S.C. §4107, Restriction on degree training

t. 5 U.S.C. §7311, Loyalty and striking

u. 5 U.S.C. §7532, Suspension and Removal

v. 18 U.S.C. §793, Gathering, transmitting, or losing defense information

w. 38 U.S.C. §501(a), Rules and Regulations

x. 38 U.S.C. §7421(a), Personnel administration; in general

y 50 U.S.C. Chapter 15, National Security, Subchapter VI, Access to Classified Information

5. DEFINITIONS: Except where a specific regulation is cited, the following terms reflect VA policy and procedures and are defined within the context of authorities and references listed in paragraph 5 of this Directive.

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

b. **Adverse Action**. For Title 5 employees, removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less. See 5 CFR §752.301. For Title 38 employees, major adverse actions are suspension, transfer, reduction in grade, reduction in basic pay, or discharge. See 38 U.S.C. §7461.

c. **Applicant**. A person being considered for employment, i.e. has received an authorized conditional offer of employment but has not yet entered on duty.

d. **Appointee**. A person who has entered on duty and is in the first year of a subject-to- investigation appointment. See 5 CFR §731.101(b).

e. **Background Investigation (BI)**. This investigation covers a ten-year period and is used for High Risk positions. It consists of a review of National Agency Check (NAC)

records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check]; a credit report covering ten years; written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

f. **Background Screening**. Background screenings consist of any type of procedure used to verify the accuracy of an individual's identification, credentials, and employment history. Screenings are not of the more comprehensive types of background investigations described in this VA directive and the associated VA Handbook 0710. 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. The level of detail for a screening is determined by each Administration and staff office. This may be applied as part of the information technology risk management process and for those positions listed in paragraph 2c, Exemptions, of this directive.

g. **Classified National Security Information**. Information that has been determined pursuant to EO 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

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

i. **Critical Sensitive**. Potential for exceptionally grave damage to the national security.

j. **Custodian**. An individual who receives classified national security information.

k. **Derivative Classification**. Derivative classification consists of incorporating, paraphrasing, restating or generating, in new form, information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance.

l. **Derivative Classifier**. A derivative classifier is a person who generates classified information from information already classified.

m. **Derogatory Information**. An issue or issues justifying unfavorable suitability or security action; or, prompting an adjudicator to request additional investigation or seek clarification for issue resolution.

n. **Eligibility**. As used in this Directive and its related Handbook, it is the state of being qualified for assignment to, or retention in, sensitive national security positions.

o. **Employee**. A person who has completed the first year of a subject to investigation appointment. See 5 CFR, §731.101(b).

p. **For Official Use Only**. A determination made by an authorized holder of sensitive information that a prospective recipient requires access to specific sensitive information in order to perform or assist in a lawful and authorized governmental function.

q. **High Risk**. Positions that have the potential for exceptionally serious impact involving duties that are critical to VA or a program mission of VA with broad scope, policy, or program authority.

r. **Information**. Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics that is owned by produced by or for, or is under the control of the United States Government. Control means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

s. **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, minimize risks associated with IT system vulnerabilities; and ensuring the security of systems and data against unauthorized or inappropriate use.

t. **Limited Background Investigation (LBI)**. This investigation covers a period of three years and is used for Noncritical Sensitive positions. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check]; a credit report covering a period of three years; written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

u. **Low Risk**. Positions with limited potential for adverse impact involving duties of limited relation to the VA mission or efficiency of the service.

v. **Minimum Background Investigation (MBI)**. This investigation covers a period of five years and is used for Moderate Risk positions. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check]; a credit report covering a period of five years; written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; and a verification of the educational degree.

w. **Moderate Risk**. Positions that have potential for moderate to serious impact involving duties of considerable importance to VA or a program mission of VA with significant program responsibilities and delivery of customer services to the public.

x **National Agency Check (NAC)**. This investigation covers a review of records in the OPM Security Investigation Index (SII) and the DOD Defense Central Investigations Index (DCII); and an FBI name check and FBI fingerprint check.

y. **National Agency Check with Written Inquiries (NACI)**. This investigation covers a period of 5 years and is used for Nonsensitive or Low Risk positions in VA. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check] and written inquiries to previous employers and references listed on the application for employment.

z. **National Agency Check with Law Enforcement and Credit Check (NACLC)**. This investigation covers a period of five years and consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check]; a credit report covering five years; and written inquiries to previous employers and references listed on the application for employment. In VA it is used for non-citizen contract personnel in Low Risk/Nonsensitive positions and the periodic reinvestigations for VA police officers.

aa. **National Security**. The national defense or foreign relations of the United States.

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

cc. **Need-to-Know**. A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

dd. **Noncritical Sensitive**. A position with the potential of some damage to serious damage to the national security.

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

ff. **Original Classification**. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

gg. **Original Classification Authority**. An individual authorized in writing, by the President, agency heads, or other officials designated by the President, to classify information in the first instance. VA has no original classification authority.

hh. **Personnel Investigation**. An investigation covering reputation, suitability, loyalty, qualifications, and other pertinent factors, conducted by personal contact, written inquiry, letter, or electronic linkage with the sources of information.

ii. **Potential Impact**. The degree to which the incumbent could impair VA's mission by violating the confidentiality or integrity of medical, financial, or other sensitive information.

jj. **Public Trust**. Public Trust positions may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding significant degree of public trust; and positions involving access to or operation or control of financial records, with a significant risk for causing damage or realizing personal gain. See 5 CFR, §731.106 (b). The term refers to high or moderate risk level.

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

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

mm. **Sensitive Information**. For purposes of this directive and VA Handbook 0710, this term is used for classified information related to national security interests and that is accessed or used by individuals in positions described in 5 CFR Part 732.

nn. **Sensitive Position**. General reference to a position whose occupant could bring about, by virtue of the nature of the position, a material adverse effect on the national security or that may require access to or knowledge of classified information pertaining to national security. See 5 CFR Part 732.

oo. **Sensitivity Designation**. The rating that determines Department and program placement based on the ability to have a material adverse effect on the national security. See 5 CFR §732.201(a).

pp. **Single Scope Background Investigation (SSBI)**. This background investigation covers a ten-year period and is used for Special Sensitive and Critical Sensitive positions. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check]; a credit report covering ten years; written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; a verification of the educational degree; a spouse/cohabitant NAC excluding an FBI fingerprint check; and verification of citizenship or legal status for foreign-born immediate family members.

qq. **Special Sensitive**. Includes any position, which the Secretary determines to be in a level higher than Critical Sensitive because of access to intelligence-related information.

rr. **Suitability**. The appropriate behavior and character required for Federal service employment. A suitability determination is based on the history of an individual's

conduct and the impact on the integrity or efficiency of the service. See 5 CFR Part 731.

ss . **Top Secret**. Information of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.