Department of Veterans Affairs
Washington, DC 20420

VA Handbook 0710
Transmittal Sheet
September 10, 2004

PERSONNEL SUITABILITY AND SECURITY PROGRAM

1. REASON FOR ISSUE: This handbook establishes procedures that implement the policies set forth in VA Directive 0710, 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; and for the management and appropriate handling of classified national security documents within VA.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This handbook describes the designation of position risk levels in accordance with 5 CFR Part 731, Suitability; and sensitivity levels as applied to positions involving national security interests in accordance with 5 CFR Part 732, National Security Positions. It addresses the personnel background investigations process in VA, and rights of employees, appointees, and applicants. 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, secure handling, transmission and storage of classified national security documents in VA.

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

4. RELATED DIRECTIVE: VA Directive 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

CONTENTS

Blank

PERSONNEL SUITABILITY AND SECURITY PROGRAM

SECTION A: PERSONNEL SUITABILITY AND SECURITY ELIGIBILITY

1. PURPOSE. This section addresses the assignment of appropriate risk level and sensitivity level designations for VA positions and the commensurate scope of background investigations. These procedures apply to applicants, appointees, employees, and contract personnel within VA, for the accomplishment of the background investigation process in a timely and consistent manner.

2. POSITION RISK AND SENSITIVITY LEVEL DESIGNATIONS. VA positions are subject to suitability considerations relating to the efficiency and integrity of the Federal service. Some Department positions also include sensitivity considerations relating to national security.

a. Suitability considerations involve the assessment and designation of a position's risk level as it affects the efficiency and integrity of the Federal service. Determining an individual's suitability for Federal employment involves considerations of a person's character and conduct that may adversely impact the service. A position's risk level may also be referred to as a position's suitability designation.

b. Sensitivity considerations involve the assessment and designation of a position's sensitivity level as it affects national security. Determining an individual's eligibility for occupying a position with national security interests involves an assessment of the potential, by virtue of the nature and sensitivity level of the position, for an individual's conduct to have an adverse impact on national security. A position's sensitivity level may also be referred to as a position's sensitivity designation.

c. All position risk level and sensitivity level designations must be recorded on VA Form 2280, Position Sensitivity Level Designation, to be filed on the permanent side of the Official Personnel Folder (OPF) or, for Title 38 employees who have personnel folders, the Merged Records Personnel Folder (MRPF). This form may be accessed through the VA's Intranet at the following address http://vaww.va.gov/vaforms and is available in Acrobat Adobe image for print and fill or in JetForm filler for those who have JetForm software loaded on their workstation.

d. The Security and Investigations Center will send a letter to appointees or employees in Public Trust or national security positions to inform each individual of the level of clearance granted and the effective date. A copy of this letter will be concurrently provided to the organization that requested and was billed for the investigation.

e. Appendix A of this handbook will be used to determine these designations.

3. SUITABILITY RISK LEVELS

a. Agency heads are directed by 5 CFR Part 731, Suitability, to designate risk levels for positions in the competitive service and the Senior Executive Service. A risk level is designated at a High, Moderate, or Low Risk level as determined by the position's potential for adverse impact on the efficiency and integrity of the service. High and Moderate Risk Levels would normally be designated as Public Trust positions. Such 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; 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 C.F.R. §731.106(b).

b. Although 5 CFR Part 731 does not apply to individuals appointed under authority of Title 38 or to Title 5 excepted service, the Department may determine personnel suitability for such positions under the authority of Executive Order 10577, Part I, Rule VI, Section 6.3(b) and 5 CFR §6.3. By VA Directive 0710, VA is extending the provisions of Part 731 to the Title 5 excepted service, Title 5/Title 38 hybrid excepted service, and employees appointed under Title 38 U.S.C., Chapters 3 (except the Under Secretary for Health), 71, or 78. VA is also extending 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. The position risk levels of High, Moderate, and Low are determined by the degree of potential for an employee in such a position to adversely impact the efficiency and integrity of the Federal service. See 5 CFR §731.106(a).

4. NATIONAL SECURITY SENSITIVITY LEVELS. These positions involve national security issues as well as suitability risk levels described in paragraph 3 of this handbook. The three designated sensitivity levels of such positions are Special Sensitive, Critical Sensitive, and Noncritical Sensitive. The misconduct of an employee in such a position could adversely affect the Department and national security. Positions that do not have these sensitivities are designated as Nonsensitive. The determination of national security positions is governed by 5 CFR Part 732, National Security Positions, which applies to positions in the competitive service, the Senior Executive Service, and where authorized by the Department, the Title 5 excepted service. By VA Directive 0710, VA is hereby extending the provisions of Part 732 to positions in Title 5 excepted service, Title 5/Title 38 hybrid excepted service, and employees appointed under Title 38 U.S.C., Chapters 3 (except the Under Secretary for Health), 71, or 78. In addition, VA is extending the criteria of Part 732 to the Under Secretary for Health and employees appointed under Title 38 U.S.C., Chapters 73 and 74.

a. **Special Sensitive**. The duties of these positions involve access to intelligence-related information designated as Sensitive Compartmentalized that is classified above the Top Secret level. Authority to access this information is granted by the Central Intelligence Agency (CIA).

b. **Critical Sensitive**. The duties of these positions involve access to Top Secret information.

c. **Noncritical Sensitive**. The duties of these positions involve access to Secret or Confidential information.

5. BACKGROUND INVESTIGATION PROCESS - SUITABILITY DETERMINATIONS. The following requirements and procedures pertain to appointee and employee suitability determinations. For those positions that may have both suitability and security eligibility considerations, the higher- level background investigation must be completed. See appendix A, paragraphs 10 and 11 of this handbook. Human Resources Management or other authorized Department officials will require all individuals to present a valid photo ID with signature or a VA ID badge when taking fingerprints. In rare instances, fingerprints taken and certified by local police departments must be mailed directly to the Security and Investigations Center, VA Central Office.

a. **Investigative Process for High Risk Positions**. For these positions, appointees, employees, and contract personnel must have a favorable determination of a Background Investigation (BI) completed by OPM. Upon notification from Human Resources Management (HRM) or other appropriate officials that individuals have been appointed to Public Trust (High and Moderate Risk) positions, the Security and Investigations Center will notify the individuals by letter of the requirements and procedures for the background investigations. HRM notifies the Security and Investigations Center, using VA Form 2280 Position Sensitivity Level Designation and VA Form 0237, Personnel Security Action Request and Certification. Background investigations must be initiated within 14 calendar days of an individual's appointment to a position. All investigative forms must be submitted to OPM within that time. See 5 CFR §736.201(c), Investigative Requirements.

(1) The individual must complete a Standard Form (SF) 85P, Questionnaire for Public Trust Positions; an SF 85P-S, Supplemental Questionnaire for Selected Positions; SF 87, Fingerprint Chart or FD 258 Fingerprint Chart; an Optional Form (OF) 306, Declaration for Federal Employment; VA Form 0710, Authorization for Release of Information; and an employment application consisting of a resume; or OF 612, Optional Application for Federal Employment.

(2) Title 38 appointees or employees may submit, as applicable, VA Form 2850, Application for Physicians, Dentists, Podiatrists, and Optometrists; VA Form 2850a, Application for Nurses and Nurse Anesthetists; VA Form 2850b, Application for Residency; or VA Form 2850c, Application for Associated Health Occupations, in lieu of the resume or OF 612.

(3) The individual must complete all forms and return them to the Security and Investigations Center within 5 calendar days of receipt.

(4) Upon receipt, the Security and Investigations Center will review the forms, complete Items A-P on the SF 85P, and forward the forms to OPM to conduct the BI.

(5) Upon completion of the BI, OPM will forward the investigative report to the Security and Investigations Center, which will adjudicate the results of the BI for compliance with 5 CFR Part 731, and determine suitability for a High Risk position.

(6) Upon a favorable determination, the Security and Investigations Center will complete the bottom portion of a VA Form 0237, Personnel Security Action Request and Certification, and return it along with the OPM Certification of Investigation to the HRM Officer to be filed on the permanent side of the OPF or, for Title 38 employees who have personnel folders, the MRPF.

(7) If derogatory information is found, the Security and Investigations Center will forward both the investigative report and a letter of referral for suitability determination to the field facility HRM Officer for a local suitability determination. If the position is in VA Central Office, these documents will be sent to the appropriate HRM Officer. The HRM Officer will forward the results of the suitability determination to the Security and Investigations Center within 30 calendar days of receipt for final disposition. The Security and Investigations Center shall make final suitability determinations for all High Risk positions within the Department. If an unfavorable determination is made, procedures in paragraph 12, Rights of VA Employees, Appointees, and Applicants, in this handbook will apply. Paragraph 12 however does not apply to contract personnel.

b. **Investigative Process for Moderate Risk Positions**. For these positions, appointees, employees, and contract personnel must have a favorable determination of a Minimum Background Investigation (MBI) completed by OPM. Upon notification from HRM or other appropriate officials that individuals have been appointed to Public Trust (High and Moderate Risk) positions, the Security and Investigations Center will notify the individuals by letter of the requirements and procedures for the background investigations. HRM notifies the Security and Investigations Center using VA Forms 2280 and 0237. Background investigations must be initiated within 14 calendar days of an individual's placement in a position. All investigative forms must be submitted to OPM within that time. See 5 CFR §736.201(c), Investigative Requirements.

(1) The individual must complete an original SF 85P, SF 85P-S, two SF 87, OF 306, VA Form 0710, and an employment application consisting of a resume or OF 612. Title 38 appointees or employees may submit, as applicable, VA Form 2850, VA Form 2850a, VA Form 2850b, or VA Form 2850c in lieu of the resume or OF 612.

(2) The individual must complete and return all forms to the Security and Investigations Center within 5 calendar days of receipt.

(3) Upon receipt, the Security and Investigations Center will review the forms, complete Items A-P on the SF 85P, and forward the forms to OPM to conduct the MBI.

(4) Upon completion of the MBI, OPM will forward the investigative report to the Security and Investigations Center, which will adjudicate the results of the MBI for compliance with 5 CFR Part 731, and make a determination for suitability to occupy a Moderate Risk position.

(5) Upon a favorable determination, the Security and Investigations Center will complete the bottom portion of a VA Form 0237and return it along with the OPM Certification of Investigation to the HRM Officer to be filed on the permanent side of the OPF or, for Title 38 employees who have personnel folders, the MRPF.

(6) If derogatory information is found, the Security and Investigations Center will forward both the investigative report and a letter of referral for suitability determination to the field facility HRM Officer for a local suitability determination. If the position is in VA Central Office, these documents will be sent to the appropriate HRM Officer. The HRM Officer will forward the results of the suitability determination to the Security and Investigations Center within 30 calendar days of receipt for final disposition. The Security and Investigations Center shall make final suitability determinations for all Moderate Risk positions within the Department. If an unfavorable determination is made, procedures in paragraph 12, Rights of VA Employees, Appointees, and Applicants, in this handbook will apply. Paragraph 12 does not apply to contract personnel.

c. **Investigative Process for Low Risk and Nonsensitive Positions**. Unless exempted under the provisions of VA Directive 0710, appointees and contract personnel appointed to Low Risk/Nonsensitive positions must be the subjects of a National Agency Check with Written Inquiries (NACI) investigation conducted by OPM. See 5 CFR §736.201(c), Investigative Requirements. HRM at VA field facilities and VA Central Office will coordinate the initiation of the NACI investigations within 14 calendar days of an individual's appointment, and make final suitability determinations for individuals in these positions. However, the initiation and adjudication of contract personnel will be handled by the Security and Investigations Center. For non-citizen contract personnel, a National Agency Check with Law Enforcement and Credit (NACLC) will be initiated by the Security and Investigations Center within 14 calendar days of the individual's placement in the position. NACLC investigations require the same forms and processes as for the NACI investigations, however with the addition of a credit check.

(1) The individual must complete an original SF 85, Questionnaire for Nonsensitive Positions, one SF 87, OF 306, and an employment application consisting of a resume or OF 612. The HRM Officer or designee will provide these forms for completion to the newly appointed individual to a Low Risk/Nonsensitive position. Title 38 appointees or

employees may submit, as applicable, VA Form 2850, VA Form 2850a, VA Form 2850b, or VA Form 2850c in lieu of the resume or OF 612.

(2) The individual must complete all forms and return them within 5 calendar days. Upon completion, the forms shall be returned to the appropriate HRM Officer who will review the forms, attach a copy of the individual's application or resume to the forms, and mail to OPM, Federal Investigations Processing Center, P.O. Box 618, Boyers, PA 16018-0618. Individuals hired under contract for these positions must submit their forms to the Security and Investigations Center, Office of Security and Law Enforcement, VA Central Office, 810 Vermont Ave., NW, Washington, DC 20420.

(3) OPM will conduct the NACI and provide the results of the investigation to the requesting office.

(4) For appointees and employees the HRM Officer or designee will review the results of the investigation in accordance with 5 CFR §731.202, Criteria, to determine suitability for employment. Upon a favorable determination, the HRM Officer will complete the Certification of Investigation that accompanies the investigation and file the certification on the permanent side of the OPF or, for Title 38 employees who have personnel folders, the MRPF. If an unfavorable determination is made, procedures in paragraph 12, Rights of VA Employees, Appointees, and Applicants, in this handbook will apply. For contract personnel, the Security and Investigations Center will review the results of the investigation and make the suitability determination. Paragraph 12 however does not apply to contract personnel.

6. BACKGROUND INVESTIGATION PROCESS – NATIONAL SECURITY ELIGIBILITY DETERMINATIONS. The following requirements and procedures pertain to applicant, appointee and employee national security eligibility determinations. For those positions that may have both suitability and security eligibility considerations, the higher level background investigation must be completed. See appendix A, paragraphs 10 and 11 of this handbook.

a. **Pre-appointment Investigative Requirements**

(1) **Special Sensitive Positions**. A Single Scope Background Investigation (SSBI) must be completed by OPM, and favorably adjudicated by the CIA prior to appointment to a Special Sensitive position. Pre-appointment investigative requirements may not be waived for these positions.

(2) **Critical Sensitive Positions**. A SSBI must be completed by OPM, and favorably adjudicated by the Security and Investigations Center prior to the individual being granted access to national security sensitive information. Pre-appointment investigative requirements may be waived in an emergency, if the Secretary finds that the delay in appointment would be harmful to national security and such finding is made part of the Department's records. Individuals may be granted access to national

security sensitive information pending completion of the SSBI only when the National Agency Check (NAC) has been completed favorably with no derogatory issues. Where a waiver for a Critical Sensitive position is authorized, the SSBI must be initiated within 14 calendar days of the individual's appointment in the position. All investigative forms shall be submitted to OPM within that time. See 5 CFR §736.201(c), Investigative Requirements.

(3) **Noncritical Sensitive Positions**. A Limited Background Investigation (LBI) must be completed by OPM and favorably adjudicated by the Security and Investigations Center. The waiver restriction is optional for positions designated as Noncritical Sensitive, see 5 CFR §732.202. Pre-appointment investigative requirements may be waived if deemed appropriate by an Under Secretary, Assistant Secretary, or Other Key Official and made part of the Department's records. Individuals may be granted access to national security sensitive information only when a NAC has been completed favorably with no derogatory issues. Where a waiver is authorized, the LBI must be initiated within 14 calendar days of the individual's appointment to the position. All investigative forms must be submitted to OPM within that time. See 5 CFR §736.201(c), Investigative Requirements.

b. **Investigative Process for Special Sensitive Positions**. Before appointment to these positions, individuals must have a favorable determination of an SSBI conducted by OPM. Upon notification by HRM of individuals selected for Special Sensitive positions, the Security and Investigations Center will notify the individuals by letter of the requirements and procedures for the background investigations. HRM will notify the Security and Investigations Center using VA Forms 2280 and 0237. The CIA is the authorized agency for making final security eligibility determinations for these positions.

(1) The individual must complete an original SF 86, Questionnaire for National Security Positions; a SF 85P-S; two SF 87, OF 306, VA Form 0710, and an employment application consisting of a resume, or OF 612. Title 38 appointees or employees may submit, as applicable, VA Form 2850, VA Form 2850a, VA Form 2850b, or VA Form 2850c in lieu of the resume or OF 612.

(2) The individual must return the completed forms to the Security and Investigations Center within 5 calendar days of receipt.

(3) Upon receipt, the Security and Investigations Center will review the forms, complete Items A-P on the SF 86, and forward the forms to OPM to conduct the SSBI.

(4) Upon completion of the SSBI, OPM will forward the investigative report to the Security and Investigations Center, which will adjudicate the results of the SSBI for compliance with 5 CFR Part 732, National Security Positions, and Executive Order (E.O.) 12968, Access to Classified Information, to determine eligibility for a Special Sensitive position. The Security and Investigations Center will then forward the investigative report to the CIA for final adjudication. If the Security and Investigations

Center makes an unfavorable determination, the investigative report is not forwarded to the CIA.

(5) Upon a favorable determination by the CIA, the Security and Investigations Center will complete the bottom portion of a VA Form 0237and return it along with the OPM Certification of Investigation to the HRM Officer to be filed on the permanent side of the OPF or, for Title 38 employees who have personnel folders, the MRPF.

(6) If the Security and Investigations Center makes an unfavorable determination, procedures in paragraph 12, Rights of VA Employees, Appointees, and Applicants, of this handbook will apply.

(7) If the investigation is not for a first-time clearance for a Special Sensitive position and the SSBI exceeds a two-year time limit, then the subject must complete an original SF 86 which the Security and Investigations Center will forward to the CIA.

(8) If the CIA makes an unfavorable adjudication, VA will withdraw its request to the CIA for the subject's clearance at the Special Sensitive level.

c. **Investigative Process for Critical Sensitive Positions**. Unless a waiver of a pre-appointment investigation has been authorized, as described in paragraph 6a(2) of this handbook, individuals selected for these positions must have a favorable determination of an SSBI prior to appointment to Critical Sensitive positions.

(1) The individual must complete an original SF 86; a SF 85P-S; two SF 87, OF 306, VA Form 0710, and an employment application consisting of a resume or OF 612. Title 38 applicants, appointees or employees may submit, as applicable, VA Form 2850, VA Form 2850a, VA Form 2850b, or VA Form 2850c in lieu of the resume or OF 612.

(2) The individual must return the completed forms to the Security and Investigations Center within 5 calendar days of receipt.

(3) Upon receipt, the Security and Investigations Center will review the forms, complete Items A-P on the SF 86, and forward the forms to OPM to conduct the SSBI.

(4) Upon completion of the SSBI, OPM will forward the investigative report to the Security and Investigations Center, which will adjudicate the results of the SSBI for compliance with 5 CFR Part 732, National Security Positions, and Executive Order (E.O.) 12968, Access to Classified Information, to determine eligibility for a critical sensitive position.

(5) Upon a favorable determination, the Security and Investigations Center will complete the bottom portion of a VA Form 0237and return it along with the OPM Certification of Investigation to the HRM Officer to be filed on the permanent side of the OPF or, for Title 38 employees who have personnel folders, the MRPF.

(6) If an unfavorable determination is made, procedures in paragraph 12, Rights of VA Employees, Appointees, and Applicants, of this handbook will apply.

d. **Investigative Process for Noncritical Sensitive Positions**. Unless a waiver of a pre-appointment investigation has been authorized, as described in paragraph 6a(3) of this handbook, individuals selected for these positions must have a favorable determination of an LBI prior to appointment to Noncritical Sensitive positions. Upon notification by HRM of individuals appointed to such positions, the Security and Investigations Center will notify these individuals by letter of the requirements and procedures for the background investigations. HRM will notify the Security and Investigations Center using VA Forms 2280 and 0237. If the LBI has not been favorably completed prior to appointment, the position may be filled when the NAC has been completed favorably with no derogatory issues. However, the LBI must be initiated within 14 calendar days of appointment in the position. See 5 CFR §736.201(c), Investigative Requirements.

(1) The individual must complete an original SF 86, SF 85P-S, two SF 87, OF 306, VA Form 0710, and an employment application consisting of a resume or OF 612. Title 38 applicants, appointees or employees may submit, as applicable, VA Form 2850, VA Form 2850a, VA Form 2850b, or VA Form 2850c in lieu of the resume or OF 612.

(2) The individual must return the completed forms to the Security and Investigations Center within 5 calendar days of receipt.

(3) Upon receipt, the Security and Investigations Center will review the forms, complete Items A-P on the SF 86, and forward the forms to OPM to conduct the LBI.

(4) Upon completion of the LBI, OPM will forward the investigative report to the Security and Investigations Center, which will adjudicate the results of the LBI for compliance with 5 CFR, Part 732 and E.O. 12968 and make a determination for eligibility to occupy a position.

(5) Upon a favorable determination, the Security and Investigations Center will complete the bottom portion of a VA Form 0237and return it along with the OPM Certification of Investigation to the HRM Officer to be filed on the permanent side of the OPF or, for Title 38 employees who have personnel folders, the MRPF.

(6) If an unfavorable determination is made, procedures in paragraph 12, Rights of VA Employees, Appointees, and Applicants, of this handbook will apply.

7. INVESTIGATIVE PROCESS FOR CONTRACT PERSONNEL

a. For suitability and security eligibility determinations within VA, contract personnel will be subject to the same investigative requirements as those for regular VA

appointees and employees. When appropriate, exemptions may be applied as described in VA Directive 0710, paragraph 2c, Exemptions. The Security and Investigations Center initiates and adjudicates background investigations of contract personnel for Low, Moderate, and High Risk position designations. Non-citizen contract personnel appointed to Low Risk or Nonsensitive positions will be subject to a NACLC investigation, to be initiated by the Security and Investigations Center within 14 calendar days of appointment.

b. Individuals with responsibility to award contracts must ascertain whether a prior background investigation was completed and is still valid on the contract personnel. If a background investigation has been completed and is still valid, the contractor must provide certification to the VA official authorized to award the contract. In turn, this information must be submitted to the Security and Investigations Center.

c. The Security and Investigations Center does not initiate nor adjudicate background investigations for contract personnel in positions with national security sensitive designations. If contract personnel are placed in such positions, the appropriate level of background investigation must be completed and on file by Defense Industrial Security Clearance Organization (DISCO) prior to entry on duty in VA.

d. Contract personnel may be provided brief or one-time access to non-national security VA information in the performance of their contract requirements without requiring a background screening or investigation. All such contract personnel will be escorted or overseen by a suitable VA employee designated by the facility or organization's ISO.

e. A risk assessment will be conducted by the requesting office and reviewed by the Information Security Officer using Appendix A and Information Technology Risk Assessments to determine the level of access required for the performance of the contractor's work. This risk assessment will examine the need and urgency of the contractor's performance, balanced against the possible harm that could result from the 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 information. The Information Security Officer will then make a written determination as to the appropriate safeguards required to protect VA information. These safeguards can range from intermittent to continuing oversight by a suitable VA employee. Such a risk assessment will also ensure that consistent procedures are taken in the protection of VA information that is non-national security in nature.

8. RISK LEVEL CHANGES. If an individual moves to a higher risk level position, or the risk level of the position itself is changed, the individual may require an upgrade

investigation. HRM will notify the Security and Investigations Center of a change to a higher risk level within one business day of the change. If an upgrade investigation is required, the investigation for that new risk level must be initiated within 14 calendar

days. The individual may encumber or remain in the position pending the completion of the background investigation. See 5 CFR 731.106(e), Risk Level Changes.

9. PERIODIC REINVESTIGATIONS

a. In accordance with 5 CFR §732.203, Periodic reinvestigation requirements, employees in Special Sensitive and Critical Sensitive positions are subject to periodic reinvestigation 5 years after placement and at least once each succeeding 5 years. HRM should notify the Security and Investigations Center whenever an employee leaves a position requiring a reinvestigation within 30 calendar days of the employee's departure.

b. In accordance with 38 U.S.C. §501 and §7421 and 5 CFR §731.106(d), Suitability Reinvestigations, employees in High Risk positions will be subject to periodic reinvestigations. VA has determined that periodic reinvestigations will be conducted 5 years after the completion date of the initial background investigation and at successive 5-year intervals.

c. Employees who occupy Noncritical Sensitive positions with access to Secret information will require periodic reinvestigations every 10 years in accordance with E.O. 12968 §3.4(c).

d. Employees who occupy Moderate Risk level positions will require periodic reinvestigations only if disqualifying suitability or sensitivity issues occur. For VA police officers, NACLC periodic reinvestigations will be conducted at 5-year intervals.

e. The Security and Investigations Center will notify employees requiring periodic reinvestigations, by letter, of the requirements and procedures for the background investigations.

f. The following reinvestigation requirements and procedures apply to those positions, as noted, with suitability and/or security eligibility considerations. The employee must complete:

(1) An original SF 86 (Special Sensitive and Critical Sensitive positions);

(2) An original SF 85P (High Risk and Moderate Risk VA police officers positions)

(3) An SF 85P-S, a VA Form 0710, and two SF 87 (all positions)

g. Return all forms to the Security and Investigations Center within 5 calendar days of receipt.

h. Upon receipt, the Security and Investigations Center will review the forms, complete Items A-P on the SF 86 or SF 85P, and forward the forms to OPM to conduct the Periodic Reinvestigation.

i. Upon completion of the Periodic Reinvestigation, OPM will forward the investigative report to the Security and Investigations Center which will adjudicate the results of the investigation in compliance with 5 CFR Part 731, or 5 CFR Part 732 and E.O. 12968, to determine the incumbent's eligibility to occupy a Critical Sensitive position; or the incumbent's suitability to occupy a High Risk, or Moderate Risk position (VA police officers). As with first-time investigations for Special Sensitive positions, the Security and Investigations Center will make an initial security eligibility determination and then forward the investigative report to the CIA for final adjudication.

j. Upon favorable determination, the Security and Investigations Center will provide the servicing HRM Officer with a letter confirming the favorable determination for continued employment. If an unfavorable determination is made, procedures in paragraph 12, Rights of VA Applicants, Appointees, and Employees, of this handbook will apply.

10. DISPOSITION OF INVESTIGATIVE FILES

a. If there are no unfavorable findings as a result of the investigation, keep a copy of the Report of Adjudicative Action (Form 79A) for two years, but destroy the rest of the investigation information. The Certificate of Investigation (CIN) should be placed in the employee's OPF or MRPF on the permanent side of the folder. A copy of the CIN may be kept with the 79A.

b. If there are unfavorable findings as a result of the investigation, keep a copy of the Report of Adjudicative Action Form (Form 79A) for two years, and keep any of the investigation information that will support the proposed adverse action. Destroy what is not applicable. Officials can extract information from the background investigation for the action and use the extractions for any due process that may follow.

c. OPM guidance requires that a copy of the Report of Adjudicative Action (Form 79A) be kept for 2 years and may be destroyed only after that period. The investigative results and 79As can be maintained in accordance with agency requirements, but no longer than OPM's retention period. The current retention period is 15 and 25 years; however, OPM is currently updating their systems notice which will reflect the retention period as 16 years and 25 years. Preferred method of destroying investigative material is by shredding.

d. VA officials can obtain a copy of an investigation file that was previously conducted for them any time within the OPM retention period. Request should be made to the Office of Personnel Management, FIPC, P. O. Box 618, Boyers, PA 16018-0618, or at (724) 794-55612.

11. DEROGATORY INFORMATION. If derogatory information on an individual who occupies a national security or Public Trust position becomes known to the facility's HRM Officer, the HRM Officer will notify the Security and Investigations Center in writing**.** The HRM Officer should be notified in writing of derogatory information from any other individual to include VA management officials or law enforcement officials. The HRM Officer must ensure a reasonable level of accuracy of derogatory information prior to notifying the Security and Investigations Center, which will review the information to determine the appropriate action.

12. RIGHTS OF VA APPLICANTS, APPOINTEES, AND EMPLOYEES. The following requirements and procedures must be followed when VA proposes to take a final suitability action against an applicant or appointee or an action against an employee based on suitability criteria, or when VA makes an adjudicative decision on national security grounds based on an OPM investigation, including changing a tentative favorable security placement or clearance decision to an unfavorable decision. This paragraph does not apply to contract personnel or volunteers.

a. **Suitability Actions**

(1) **Covered positions**

(a) **Title 38 Health Care Applicants, Appointees, and Employees (and the Under Secretary for Health).** Suitability determinations and procedural protections for Title 38 applicants, appointees, and employees appointed under 38 U.S.C. §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.

(b) **Applicants, Appointees, and Employees in the Title 5 Excepted Service, the Title 5/Title 38 Hybrid Positions, and under Title 38, Chapters 3 (except the Under Secretary for Health), 71 or 78**. Suitability determinations and procedural protections for these individuals are outlined in subparagraph 12 a (2).

(c) **Title 5 Competitive Service Positions and Career Appointment in the Senior Executive Service (hereinafter competitive service).**

1. **Applicants and appointees (See VA Directive, paragraphs 5.c and 5.d.).** OPM has delegated to agencies limited authority for adjudicating suitability for applicants and appointees in the competitive service. See 5 CFR § 731.103(a). Under its delegated authority, VA may take a suitability action against an applicant or appointee based on the criteria of 5 CFR § 731.202 subject to the limitations prescribed in 5 CFR § 731.103. See 5 CFR § 731.105(b). OPM retains jurisdiction in all competitive service cases involving evidence of material, intentional false statement or

deception or fraud in examination or appointment. See 5 CFR § 731.103(a). VA must refer these cases to OPM for adjudication, or contact OPM for prior approval if the Department wants to take action under its own authority under 5 CFR Parts 752 or 315. In addition, cases that involve refusal to furnish testimony as required by 5 CFR § 5.4, or pass-over requests involving preference eligibles who are 30 percent or more compensably disabled, must be referred to OPM for adjudication. See 5 CFR § 731.103(a). OPM also may take a suitability action against an applicant or appointee based on any of the criteria of 5 CFR § 731.202. See 5 CFR § 731.105(a).

2. **Employees (See VA Directive 5.o.).** OPM may take a suitability action against an employee only in cases involving evidence of material, intentional false statement or deception or fraud in examination or appointment, or refusal to furnish testimony as required by 5 CFR § 5.4, or statutory or regulatory bar. See 5 CFR § 731.105(c). VA must refer these cases to OPM for adjudication, or obtain prior approval from OPM before VA can take an action under 5 CFR Parts 752 or 315. VA does not have delegated authority to take a suitability action against an employee. See 5 CFR § 731.105(d). However, VA is not precluded from taking an action against an employee under the procedures set forth in 5 CFR Parts 752 and 315, based on suitability criteria. If an action based on suitability criteria is taken against an employee under 5 CFR Parts 752 or 315, the employee may submit a written request for a copy of the disqualifying information from the Security and Investigations Center. The employee may obtain a copy of the investigative report by writing to Office of Personnel Management, Federal Investigations Processing Center, P.O. Box 618, Boyers, PA 16018-0618.

(2) **Suitability Action Procedures.**

(a) If OPM instructs VA to take a suitability action against an applicant, appointee or employee, then the procedures specified in 5 CFR §§731.301-731.304, as appropriate, must be followed.

(b) If VA, other than the Office of Inspector General (OIG), takes a suitability action under its delegated authority against an applicant or appointee, the following procedures must be followed: Note: If the OIG takes a suitability action under its delegated authority for applicants and appointees in the OIG, suitability action procedures will be provided by the Inspector General.

1. Notice of Proposed Action. The Office of Security and Law Enforcement, Security and Investigations Center (for Public Trust positions) or the Human Resources Office (for Low Risk/Nonsensitive positions) shall provide an applicant or appointee with reasonable notice in writing of a proposed final suitability action and the charges against them. The notice will state the specific reasons for the proposed action; the right to respond in writing; the time limits for the response as well as the address to which the response is made; and the availability for review, upon request, of the materials relied upon. If the respondent is employed in the competitive service on the date the notice is

served, he or she is entitled to be retained in a pay status during the notice period. See 5 CFR §731.402.

2. Answer. The applicant or appointee may respond to the charges in writing including any other necessary documentation or affidavits that support the response. See 5 CFR § 731.403.

3. Decision. The agency's decision shall be in writing and inform the applicant or appointee of the reasons for the decision. The individual will also be informed of appeal rights with the Merit Systems Protection Board (MSPB). See 5 CFR §731.404, §731.501(a)-(b), §731.103(g), and 5 CFR Part 1201. The employing office shall remove an appointee from the rolls within five workdays of the final decision.

b. **National Security Eligibility Actions**

(1) **Covered Positions**. Ineligibility determinations made in the interest of national security are covered by 5 CFR Part 732, which applies to the competitive service, the Senior Executive Service, and, where authorized by the agency, to the excepted service. See 5 CFR § 732.102(b). VA Directive and Handbook 0710, Personnel Suitability and Security Program, extend the provisions of 5 CFR Part 732 to individuals appointed to the Title 5 excepted service, Title 5/Title 38 hybrid positions, and employees appointed under Title 38 U.S.C. Chapters 3 (except the Under Secretary for Health), 71 or 78; and 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.

(2) **National Security Eligibility Action Procedures.** When VA makes an adjudicative 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 5 CFR §732.301. 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 are accurate, relevant, timely, and complete to the extent reasonably necessary to ensure fairness to the individual; comply with all applicable administrative due process requirements, as provided by law, rule or regulation; consider all available information in reaching its final decision; and keep any record of the agency action required by OPM. The Secretary or designee may revoke a security clearance and remove an employee under 5 U.S.C. 7532 where it is necessary in the interests of national security. The Secretary also may take an adverse action under 5 USC 7512-13 or subchapter 5 of Chapter 74 of title 38, U.S.C., as appropriate against an employee for loss of a security clearance, if required for the position.

(a) **Denials or Revocations of Security Clearances.** When action is taken to withhold or revoke a security clearance, the following due process must be provided to

applicants or employees, pursuant to Executive Order 12968, Part 5, unless the Secretary determines that the procedures cannot be invoked in a manner that is consistent with national security:

1. 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;

2. 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. If requested, any documents, records and reports upon which the denial or revocation is based must be provided within 30 days, to the extent permitted by the national security and other applicable law, and the entire investigative file must be provided prior to the time set for a written reply.

3. Reasonable opportunity to reply in writing to, and to request a review of, the determination;

4. Written notice of and reasons for the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

5. An opportunity to appeal in writing to a high level panel, appointed by the Secretary, which shall be comprised of at least three members, two of whom shall be selected from outside the security field.

6. An opportunity to appear personally and to present relevant documents, materials, and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the Secretary. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record. Where such appearance occurs before the appeals panel, a written summary may be made.

7. The decision of the appeals panel shall be in writing, and 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 shall be final.

8. Any procedure set forth in subparagraphs 12(b)(2)(b) 1 –7 will not be made available in a particular case, where the Secretary or Deputy Secretary personally certifies that such procedure would damage the national security by revealing classified information.

(b) **Suspension and removal on national security grounds**

1. Suspension. Under 5 U.S.C. § 7532(a), the Secretary or designee may suspend an employee without pay when that action is necessary in the interests of national security. To the extent the Secretary or designee determines the interests of national security permit it, the suspended employee shall be notified of the reasons for the suspension. Within 30 days after the notification, the suspended employee is entitled to submit statements or affidavits to show why duty status should be restored.

2. Removal. 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. An employee who has a permanent or indefinite appointment, has completed the probationary or trial period, and is a citizen of the United States is entitled, after suspension and before removal, to the procedures specified in 5 U.S.C. § 7532(c).

3. Decision**.** The determination by the Secretary or designee that removal is necessary or advisable in the interests of national security is final. An individual who has been determined ineligible for a sensitive national security position may not appeal the decision to the MSPB. See 5 U.S.C. §7532(c).

(c) **Adverse action based on loss of security clearance**. Where an employee has lost a security clearance that is required for the position, VA may take an adverse action against the employee for "cause" under 5 U.S.C. 7512-13 or subchapter 5 of title 38 U.S.C. Chapter 74, as appropriate. When an adverse action is taken under 5 U.S.C. 7512-13 as a result of the loss of a security clearance, the employee is entitled to the procedural protections specified in 5 U.S.C. § 7513. However, the merits of the underlying security clearance determination may not be appealed to the MSPB. When an employee appointed under title 38 U.S.C. Chapter 74 has lost a security clearance that is required for the position, VA may take an adverse action against the employee under subchapter 5 of title 38 U.S.C. Chapter 74. The employee is entitled to the procedural protections specified therein. An employee appointed under 38 U.S.C. Chapter 73 who is removed for "cause" is subject to the applicable separation procedures outlined in VA Directive and Handbook 5021, Employee/Management Relations.

SECTION B: CLASSIFIED DOCUMENT SECURITY

1. PURPOSE. This section implements Executive Order (E.O.) 12958, Classified National Security Information, as amended by E.O. 13292 and E.O. 12968, Access to Classified Information and policy set forth in VA Directive 0710, Personnel Suitability and Security Program. It provides mandatory procedures for handling, transmitting, and storing classified national security documents.

2. SECURITY EDUCATION. The Security and Investigations Center will ensure that initial, refresher, and termination security briefings are conducted on a regular basis. An employee granted access to classified national security documents will be briefed on the inherent responsibilities and proper procedures for handling classified national security documents and execute a SF 312, Classified Document Nondisclosure Agreement. Annual refresher security briefings will be made available for each employee. Upon termination of the individual's security clearance, either by separation, transfer, or change in duties, each employee will receive a security debriefing explaining the continuing responsibility to protect the level of information to which the individual had access.

3. REPORTING REQUIREMENTS. HRM Officers at field facilities are responsible for providing the following information on station letterhead to the Security and Investigations Center no later than October 10th of each year:

a. Information Security Oversight Office (ISOO) Report number IRCN 0230-GSA-AN, Agency Information Security Program Data, which covers the period of October 1st through September 30th each year in accordance with E.O. 12356, National Security Information and ISOO Directive No. 1.

b. An inventory of Top Secret, Secret, and Confidential documents on hand as of September 30th. Inventory must include the date of the document, classification level, name of classifier, and the location of the storage container. The outer envelope of the report should be stamped “FOR OFFICIAL USE ONLY.” The title, subtitle, or any other citation of a document should not be used on the outer envelope if it compromises the security of the classified contents.

4. ACCESS REQUIREMENTS

a. The number of personnel cleared for access to classified national security documents will be kept to a minimum.

b. Individuals who have a need to know will possess a valid security clearance. VA Form 0237, Personnel Security Action Request and Certification, will be filed in the employee's OPF or MRPF indicating that the individual has been granted access at the appropriate classification level. Security clearances are based upon the position's

sensitivity designation and an individual's need-to-know for the accomplishment of a program's mission.

c. Access by historical researchers and former presidential appointees may be granted if they are engaged in historical research projects or had previously occupied policy-making positions to which the President appointed them.

d. Waivers may be granted only if the Secretary, an Under Secretary, Assistant Secretary, or Other Key Official:

(1) Determines, in writing, that access is consistent with the interest of national security, see Section A, paragraph 6a of this handbook;

(2) Takes appropriate steps to protect classified documents from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with the National Archives and Records Administration (NARA) ISOO Directive No. 1; and

(3) Limits the access granted to former presidential appointees to items that the person originated, reviewed, signed, or received while serving as a presidential appointee.

5. ESTABLISHING CLASSIFIED CONTROLS

a. The Security and Investigations Center is the central control in VA for safeguarding and facilitating the handling and transmission of classified documents. It will maintain VA Form 4245, Classified Document Accountability Record, for all Top Secret, Secret, and Confidential documents; and exercise control over the flow of classified documents and material to ensure proper protection, accountability, and disposal in accordance with this handbook.

b. HRM Offices:

(1) Ensure that all employees who require access to classified documents are cleared by the Security and Investigations Center;

(2) Maintain liaison with the Security and Investigations Center regarding policy and procedural matters pertaining to the safeguarding of classified documents.

6. HANDLING OF CLASSIFIED DOCUMENTS

a. VA Form 4245 will be placed on top of each classified document in order to account for such documents, and remains with the document throughout its use. The Security and Investigations Center maintains the retention cycle and copy of the VA Form 4245. The entire package consisting of the classified documents and the VA

Form 4245 is hand-carried to the Security and Investigations Center for permanent storage or destruction. Within Central Office, all classified national security documents received will be immediately hand-carried to the Security and Investigations Center.

b. If hand carrying of classified documents outside of the VA building is necessary, the Security and Investigations Center must be contacted for specific instructions.

7. CLASSIFICATION LEVELS. Document classification markings are Top Secret, Secret, or Confidential. An original classifier appointed by the President classifies information. VA does not have the authority to originally classify national security information.

8. IDENTIFICATION AND MARKINGS. The original classification authority shall mark by stamp, typewriter, or ink the following information on the cover sheet and first page of all classified documents:

a. One of the three classification levels;

b. The identity, by name or personal identifier and position, of the original classification authority;

c. The agency and office of origin;

d. Declassification instructions, which shall indicate one of the following:

(1) The date or event for declassification; or,

(2) The date that is 10 years from the date of original classification, or

(3) The exemption category from declassification;

e. A concise reason for classification.

9. DECLASSIFICATION AND DOWNGRADING. Documents will be declassified or downgraded only by the original classifier or successor official.

10. STORAGE AND HANDLING OF CLASSIFIED DOCUMENTS. Top Secret, Secret, and Confidential documents will be stored in a General Services Administration (GSA)-approved safe or vault having a built-in, three-position dial combination lock.

11. CONTAINER ASSIGNMENT NUMBERS AND COMBINATIONS

a. **Containers**. Security containers will be numbered and SF 700, Security Container Information, completed. The container number, posted in Block 5 of SF 700, will also be posted on the exterior front side of the container.

b. **Classifying Combinations**. Upon receipt of a storage container, the factory preset combination will be changed and recorded on an SF 700 which then becomes a classified document. Classified combination documents will be declassified immediately upon change of combination and completion of a new SF 700. The markings on the old SF 700 will be destroyed by shredding.

c. **Recording Storage Facility Data**. SF 700, Part 1, will be posted on the inside of the top drawer of the security container. SF 700, Parts 2 and 2A will bear classification markings of the highest level of classified documents authorized for storage. After Part 2A is completed and marked with appropriate classification markings, it will be enclosed and sealed in the form's attached envelope.

d. **Custodians**. Since the custodians' personal data on SF 700 will be posted inside the classified container and at the Security and Investigations Center, their home address and telephone number will not be available to the public.

e. **Combinations**

(1) Combinations to classified containers will not be retained on one's person, in a wallet or purse, or entered on a calendar, calendar pad, desk drawer, in a calculator, or any similar unauthorized location. Combinations are to be memorized by authorized and alternate custodians. The only authorized combination record is on SF 700, maintained by the Security and Investigations Center.

(2) Combinations will be changed only by authorized vendors and will be changed when:

(a) Placed in use;

(b) An individual knowing the combination no longer requires access to the combination;

(c) Whenever a combination has been subjected to possible compromise; or

(d) At least every year.

f. **Unused Security Containers**. When a security container is no longer in use, the combination shall be set at the standard combination of 50-25-50. The Security and

Investigations Center shall be notified promptly in order to arrange for removal of the container.

12. FUNCTIONS OF CUSTODIANS

a. Custodians will not remove classified documents or material from authorized work areas for work at home or elsewhere during or after working hours. Such removal is not authorized.

b. Custodians will ensure that:

(1) Classified documents removed from classified containers are covered by the appropriate classification cover sheet; SF 703, Top Secret Cover Sheet, SF 704, Secret Cover Sheet, or SF 705, Confidential Cover Sheet.

(2) Classified containers are not left unlocked and unattended by personnel who do not have a security clearance equivalent to the highest level of classification authorized for storage.

(3) Combinations are changed, recorded, and disseminated as listed under paragraph 11, above.

(4) Appropriate locking and checking functions are accomplished each workday.

13. CARE DURING WORKING HOURS. A classified document removed from storage will be appropriately covered using a SF 703, SF 704, or SF 705. The cover labels may be removed prior to dispatch by mail. To save space in classified security containers, cover labels may be removed prior to storage of classified material in classified container.

14. END-OF-DAY SECURITY CHECKS

a. The custodian who unlocks a classified security container will enter the date, his/her initials, and time in the appropriate blocks of SF 702, Security Container Checklist. The custodian will lock the container whenever the container will not be attended by suitably cleared employees or at the close of the workday. The person locking the container will rotate the dial of the combination lock a minimum of four complete turns in the same direction, not back and forth, and then attempt to operate each door, drawer, or opening by trying to operate each knob, lever, latch, or handle. The custodian will then enter his/her initials and the time in the appropriate blocks of SF 702.

b. At the end of the workday, or following the final closing of the classified security container, a custodian other than the one who locked the container will complete the same actions indicated in paragraph 14a of this handbook.

c. Checking is required for each normal workday, whether or not the security container was opened. If the container was not opened, the custodian will enter "Not Opened" adjacent to the date under the "Opened By" and "Closed By" columns on the SF 702; complete the checks indicated in paragraph 14a of this handbook, and enter his/her initials and the time in the "Checked By" column.

d. The individuals assigned to that work area at the end of normal duty hours will inspect the area where classified documents are developed or used. The inspection must reflect that:

(1) All classified material is in secure storage or under the care of the authorized individual in the same room or area.

(2) SF 701, Activity Security Checklist, is completed in connection with these close-of-business checks. Other entries such as lights off, appliances unplugged, or other equipment turned off may be added to the checklist.

(3) SF 701 and SF 702 may be destroyed on the first duty day of the following month, unless a preliminary inquiry or investigation involving that classified container or area is in progress.

15. TRANSMITTAL

a. **Transmittal of Classified Documents**. Classified documents will be enclosed in an inner and outer cover before transmitting. The inner cover will be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover will be sealed and addressed with no identification of the classification of its contents. A receipt will be attached to or enclosed in the inner cover, except that confidential documents shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, addressee, and the document but will contain no classified documents. It will be immediately signed by the recipient and returned to the sender.

b. **Transmittal of Top Secret Documents**. The transmittal of Top Secret documents will be by State Department diplomatic pouch, by a messenger-courier system specifically created for that purpose, or other authorized secure communications circuits. The Security and Investigations Center maintains a list of such authorized individuals.

c. **Transmittal of Secret Documents.** The transmittal of Secret material will be in the following manner:

(1) Within the U.S., District of Columbia, and Puerto Rico. Secret documents may be transmitted within and between the 50 States, the District of Columbia, and Puerto Rico by one of the means authorized for Top Secret material, by U.S. Postal Service registered mail, or by protective services provided by U.S. air or surface commercial carriers.

(2) Other Areas. Secret documents may be transmitted from, to, or within areas other than those specified above by one of the means established for Top Secret documents. It may also be transmitted by U.S. registered mail through Army, Navy, or Air Force Postal Service facilities provided that the material does not pass through a foreign postal system. Transmittal outside such areas may also be accomplished under escort of appropriately cleared personnel aboard U.S. Government and U.S. Government contract vehicles or aircraft, ships of the U.S. Navy, civil service manned U.S. Naval ships, and ships of U.S. Registry. Operators of vehicles, captains or masters of vessels, and pilots of aircraft who are U.S. citizens and who are appropriately cleared may be designated as escorts.

d. **Transmittal of Confidential Documents**. Confidential documents will be transmitted within and between the 50 States, the District of Columbia, Puerto Rico, and U.S. territories or possessions by one of the means established for Secret or Top Secret material or by U.S. Postal Service certified, first-class, or express mail service. Outside these areas, confidential documents will be transmitted only as it is authorized for Secret or Top Secret documents.

16. LOSS OR POSSIBLE COMPROMISE. Any person who has knowledge of the loss or possible compromise of classified national security documents within VA will immediately report the circumstances to Security and Investigations Center. In turn, the originator will be notified. An immediate inquiry will be initiated by the Security and Investigations Center for the purpose of taking corrective measures and appropriate administrative, disciplinary, or legal action.

17. DESTRUCTION OF CLASSIFIED DOCUMENTS. Classified documents that have served the intended purpose will be shred in a GSA-approved shredder for classified material.