GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

ADM 9732.1E
March 12, 2019

GSA ORDER

SUBJECT: Personnel Security and Suitability Program Handbook

1. Purpose. To issue an updated U.S. General Services Administration's (GSA) Personnel Security and Suitability Program Handbook.

2. Background. The Personnel Security and Suitability Program responsibilities and procedural requirements for investigations, suitability adjudications, security clearance determinations, and appeals of GSA employees, applicants, appointees, volunteers, and affiliates, are all updated. These Federal requirements are a result of various sources including:

a. Executive Order (EO) 12968, as amended, Access to Classified Information (August 2, 1995);

b. EO 13467, as amended, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (June 30, 2008);

c. EO 13488, as amended, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust (January 16, 2009);

d. EO 13526, as amended, Classified National Security Information (December 29, 2009);

e. EO 13764, Amending the Civil Service Rules, EO 13488, and EO 13467 to Modernize the Executive Branch-wide Governance Structure and Process for Security Clearance, Suitability and Fitness for Employment, and Credentialing, and Related Matters (January 17, 2017);

f. 5 Code of Federal Regulations (CFR) Part 731 - Suitability;

g. 5 CFR Part 732 - National Security Positions;

h. 5 CFR Part 736 - Personnel Investigations;

i. 5 CFR Part 1400 - Designation of National Security Position;

j. Homeland Security Presidential Directive-12 (HSPD-12) - Policy for a Common Identification Standard for Federal Employees and Contractors, as it applies to GSA (August 27, 2004);

k. Security Executive Agent Directive (SEAD) 3. Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position (June 12, 2017);

l. SEAD 4. National Security Adjudicative Guidelines (June 8, 2017);

m. SEAD 6. Continuous Evaluation Program (January 12, 2018); and

n. n. SEAD 7. Reciprocity of Background Investigations and National Security Adjudications (November 9, 2018).

3. Scope and applicability.

a. This Order describes the investigations program as it applies to GSA. In addition, commissions, committees, and other entities supported by GSA may use this Handbook for guidance. Nothing in this Policy is intended to limit the independent authority of the Office of Inspector General (OIG) under the Inspector General Reform Act with regard to OIG's programs and personnel.

b. GSA employs only persons who are suitable for employment (5 CFR Part 731), and grants national security clearances only to persons whose employment is clearly consistent with the national security interest (5 CFR Part 732). Unless the U.S. Office of Personnel Management (OPM) grants specific exceptions, all GSA employees must undergo personnel security investigations (5 CFR Part 736). GSA makes National Security and Suitability determinations based on current and relevant prior security investigations, and other investigative materials (criminal, employment, and credit history, etc.) that are developed during the vetting process.

4. Cancellation. The Order cancels and supersedes ADM P 9732.1D.

5. Policy. GSA requires all personnel to have the ability to receive and maintain a favorably adjudicated background investigation at the level required by their Position Description.

6. Nature of revision. This Handbook is revised to:

a. Provide guidance for further implementation of Executive Order 13488, as amended, for reinvestigating persons in positions of Public Trust (high and moderate risk levels) and granting reciprocity.

b. Provide specific guidance for fingerprint submissions for applicants prior to entry on duty (EOD).

c. Require the GSA Office of Human Resources Management (OHRM) to use the OPM Position Designation Automated Tool to determine the position risk and sensitivity levels and to identify the background investigation required for the position as part of the hiring process and prior to placement.

d. Continue to require a completed favorable background investigation in order to have full access to GSA facility and information technology (IT) systems. GSA will issue an identity credential providing limited access to GSA facility and IT systems following the initiation of an investigation and the favorable adjudication of the fingerprint results.

e. Introduce the Continuous Evaluation (CE) process. CE is a Director of National Intelligence (DNI) established program that is part of the security clearance reform effort to improve personnel security processes and increase the timeliness of information reviewed between periodic reinvestigation cycles.

f. Information regarding contract employees, previously covered in ADM 9732.1D is now located in GSA Order ADM 5400.2, General Services Administration Heads of Services and Staff Offices' and Requesting Officials' Roles and Responsibilities to Implement Homeland Security Presidential Directive-12.

g. Introduce changes in the designation of Public Trust and National Security positions to the Tiered Investigation Standards in accordance with EO 13467, as amended, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information.

7. Signature.

_____
EMILY W. MURPHY
Administrator

ADM 9732.1E Personnel Security and Suitability Program Handbook
Table of Contents

CHAPTER 1

PERSONNEL SECURITY AND SUITABILITY PROGRAM

1. Practice. GSA is responsible for implementing a comprehensive and effective Personnel Security and Suitability Program. The Program:

a. Evaluates the character and conduct of applicants and appointees for the purpose of making suitability determinations for covered positions and continuous evaluation through ensuring timely reinvestigations of employees in positions of public trust as required by EO 13488, as amended, Granting Reciprocity on Excepted Service and Reinvestigating Individuals in Position of Trust, and 5 CFR Part 731, Suitability.

b. Evaluates the character and conduct of employees for excepted service or other non-covered positions.

c. Determines the eligibility of employees for national security positions under EO 13764, Amending the Civil Service Rules, EO 13488, and EO 13467 to Modernize the Executive Branch-wide Governance Structure and Process for Security Clearance, Suitability and Fitness for Employment, and Credentialing, and Related Matters, the eligibility for access to classified information under EO 12968, as amended, Access to Classified Information; EO 13526, as amended, National Security Information, and 5 CFR Part 1400, Designation of National Security Positions.

2. Responsibilities. The authorities cited above require the GSA Administrator to have a Personnel Security Program. To meet these responsibilities, the GSA Administrator designated the Associate Administrator of the Office of Mission Assurance (OMA) to implement and maintain the program. The Heads of Services and Staff Offices (HSSOs), as well as the Administrator and Regional Administrators (RAs), must follow this Handbook and ensure coordination between personnel security and personnel practices.

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

b. The OMA Associate Administrator assigned to the OMA Personnel Security Branch responsibility in GSA for:

(1) Requesting investigations on candidates for Low, Moderate and High Risk Public Trust positions, and all National Security positions;

(2) Storing all materials and information relating to personnel investigations in GSA. The Personnel Security Branch is the only authorized storage location for such materials in GSA;

(3) Verifying all investigations and security clearances passed for visitor access.

(4) Making all decisions to grant, suspend, revoke, or deny National Security clearances. These decisions can be appealed in accordance with the Due Process procedures outlined in Appendix I;

(5) Granting waivers of pre-appointment investigations for National Security positions for a limited period, if the GSA Administrator finds that such action is necessary in the national interest. Pursuant to 5 CFR 732.202, the pre-appointment investigative requirement **may not** be waived for appointment to positions designated Special-Sensitive;

(6) Safeguarding reports, records, and files pertaining to adjudicative matters. This information must be maintained in confidence and disseminated only to authorized officials in GSA who have a clear, official need to review the material;

(7) Surveying, training, or inspecting all GSA organizations to ensure compliance with this Handbook (re-investigations, refresher training, briefings, and debriefings); and

(8) Ensuring that all information collected is protected in accordance with the Privacy Act of 1974.

(9) Granting certifications of investigations for national security clearances and public trust positions.

c. The HSSOs are responsible for:

(1) Identifying National Security Positions in their organizations;

(2) Coordinating with their servicing OHRM and the Personnel Security Branch to ensure that GSA requests the appropriate investigations on all appointees before they enter on duty;

(3) Complying with the policies, guidance, and direction set forth in this Handbook; and

(4) Notifying the Personnel Security Branch of employees in National Security or Public Trust Positions who engage in possibly disqualifying conduct listed in Appendix C.

d. OHRM is responsible for:

(1) Arranging for all appointees (new and transferred) to complete the appropriate investigative forms;

(2) Conducting initial screening of the investigative forms;

(3) Bringing new employees into positions designated Special-Sensitive only after the Personnel Security Branch has certified their investigation;

(4) Bringing new employees on board into Critical-Sensitive positions only after the Personnel Security Branch has certified their investigation or waived this requirement;

(5) Bringing all other new employees on board only after the Personnel Security Branch notifies OHRM that the advance fingerprint checks are favorable;

(6) Notifying the Personnel Security Branch when new employees will enter on duty; and

(7) Certifying that employees who are due for re-investigations in public trust and national security positions are still assigned to those positions.

e. Adjudicators will:

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

(2) Meet the requirements of the National Training Standards issued by OPM and the Office of the Director of National Intelligence prior to rendering an adjudicative determination; and

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

3. Certifications, reciprocity, suitability, continuous evaluation, and visit requests.

a. Certifications.

(1) National security positions. The Personnel Security Branch generates an automated form as written verification that the investigative and adjudicative criteria have been met in order for a person to occupy a national security position. Only the Personnel Security Branch may issue certifications for national security positions and grant national security clearances. The original certificates are emailed to the GSA's OHRM Consolidated Processing Center (CPC) to be placed in the official personnel folder.

(2) Public trust positions. The Personnel Security Branch generates an automated form as written verification that the investigative and adjudicative criteria have been met in order for a person to occupy a public trust position. Only the Personnel Security Branch may issue certifications for public trust positions. The

original certificates are emailed to OHRM CPC to be placed in the official personnel folder.

(3) Low risk positions. The Personnel Security Branch generates an automated form as written verification that the investigative and adjudicative criteria are met in order for a person to occupy a low risk position. Only the Personnel Security Branch may issue certifications for low risk positions. The original certificates are emailed to the OHRM CPC to be placed in the official personnel folder.

b. Reciprocity.

(1) National Security Clearances. When a person transfers to GSA from another Federal agency and has a current investigation that meets the standard to grant a security clearance, the Personnel Security Branch can use the investigation to grant the clearance, without requiring new or redundant investigations In order for the Personnel Security Branch to use any previous investigation, the investigation must have been conducted within the past 7 years and the candidate must not have more than a 2-year break in Federal employment. The previous investigations must meet current standards set by applicable Executives Orders, SEAD's, and OPM policy.

(2) Suitability investigations.

(a) Certified personnel investigations and adjudications that meet the criteria in 5 CFR 731.202 standards will be accepted from all agencies.

(b) A covered employee, as defined in Appendix J, with a break in Federal service less than 2 years does not need a new investigation. The prior investigation must meet or exceed the requirement for the position designation and have been completed within the last 5 years. In all cases, the person must complete the Optional Form 306 and submit a resume for review by the Personnel Security Branch.

(c) An excepted service employee without a break in Federal service will be granted reciprocity if the prior investigation meets or exceeds the requirement for the position.

(d) Applicants with any prior criminal record will be considered in accordance with 5 CFR 731.202.

c. Continuous evaluations (CE). All covered employees shall be subject to continuous review under standards directed by the Office of the Director for National Intelligence (ODNI). The program applies to all covered employees assigned to a sensitive position (Top Secret / Secret National Security Clearance) or having access to classified information or material. CE will include search of records of the U.S. Department of Justice, Federal Bureau of Investigation (FBI), and other databases to flag security relevant information. CE involves an ongoing assessment of an individual for retention of a security clearance or continued eligibility to hold a sensitive position.

CE provides the same information reviewed during initial and periodic reinvestigations (such as foreign travel, financial activity, and criminal activity), but on a more frequent and continuing basis.

d. GSA visit requests. A visit request is a statement completed by the Personnel Security Branch to a Federal agency or secure site that certifies the status of a personnel investigation or national security clearance for a GSA employee. All visit requests will be submitted to gsa.securityoffice@gsa.gov on GSA Form 6102, Passing Visit Authorization Letter/Request. Only the Personnel Security Branch can submit a visit request for GSA employees. The request consists of:

(1) The period of time for a visit request, which can range from a single visit to recurring visits over a period of time but not to exceed 1 year;

(2) Employee's name, date of birth, place of birth, and Social Security number;

(3) Country of citizenship;

(4) Date and level of national security clearance or public trust certification (only the Personnel Security Branch can provide this information);

(5) Type of background investigation, investigating agency, and date of investigation (only the Personnel Security Branch can provide this information); and

(6) Information on the visit which includes the facility to be visited, duration of visit, purpose, and point of contact to include name, telephone number, and the visiting agency’s Security offices unclassified fax and phone number.

CHAPTER 2

SUITABILITY

1. Suitability. 5 CFR Part 731 requires GSA to implement a suitability program for covered positions. In addition, Presidential commissions, committees, and other Federal agencies supported by GSA may use this Handbook for guidance. (This program is separate from the National Security Program in Chapter 3 of this Handbook.) Suitability refers to character and to behavior; it does not include a person's qualifications, such as experience or ability. All GSA employees must meet the suitability standard and criteria described in 5 CFR Part 731, Subpart B. To determine if persons satisfy the suitability criteria, risk levels are assigned to positions and investigations are requested for candidates under 5 CFR Part 731, Subpart A.

2. Responsibilities.

a. Personnel Security Branch. The Personnel Security Branch is responsible for the GSA Suitability and Personnel Security Program. The Personnel Security Branch requests investigations for all positions. All investigations must be initiated with OPM within 14 calendar days of placement in a position in accordance with 5 CFR Part 736. Investigations will be adjudicated by the Personnel Security Branch after a case is closed at OPM.

b. OHRM, RA, HSSO, and Executive Services. Cooperation from OHRM, Regions, HSSOs, and Executive Services is required in order to meet the OPM requirement.

3. How the suitability program works.

a. Position risk levels. In compliance with the Position Designation Automatic Tool, GSA assigns one of three risk levels to each position. The level determines what investigation is required for the position. OHRM designates the risk level for all occupations in GSA and incorporates the risk level in the position designation for each series and grade.

b. Investigations to determine suitability.

(1) The Personnel Security Branch requests investigations for all GSA personnel. The OPM National Background Investigation Bureau (OPM/NBIB) completes and returns all reports of investigations to the Personnel Security Branch for adjudication.

(2) The Personnel Security Branch receives investigations and other reports on GSA employees who may have engaged in disqualifying conduct. In such cases, the Personnel Security Branch will review the information, conduct any additional investigation necessary to resolve issues, and determine if the employee continues to

be suitable to perform the duties of the position.

(3) The Personnel Security Branch will ensure that suitability actions are handled in accordance with the requirements in 5 CFR 731.202.

(4) A suitability action is an outcome taken by OPM or GSA following an unfavorable suitability determination. Suitability actions are:

(a) Cancellation of eligibility;
(b) Removal;
(c) Cancellations of reinstatement eligibility; or
(d) Debarment.

c. Suitability determinations.

(1) Making determinations. The Personnel Security Branch will adjudicate suitability determinations using the criteria in 5 CFR 731.202 (See Appendix B for guidance in making determinations).

(2) The Personnel Security Branch makes all suitability decisions for:

(a) Unfavorable or derogatory information. If a Security Specialist cannot make a favorable determination based on 5 CFR 731.202, the specialist will send the individual a proposed action letter and the individual must provide a written answer no more than 30 calendar days after the date of the notice of proposed action. This letter will outline the issues and offer the person an opportunity to explain, refute, and/or mitigate the issues in writing. A final determination will be made after the person either replies or the 30 calendar days have passed. Any adverse actions must be reported to OPM as soon as possible but no later than 90 calendar days after receipt of the investigative report in accordance with 5 CFR 731.203.

(b) Appeal rights. Individuals will be instructed in the final letter of the appeal process to the Merit Systems Protection Board as provided for in 5 CFR Part 731.

(3) Record of determination. OPM/NBIB provides a certificate with all investigations to be completed and placed in the Electronic Official Personnel Folder (e-OPF) after the adjudication is completed. OPM/NBIB will also provide the Report of Agency Adjudicative Action (INV) Form 79A for GSA to complete and return to OPM/NBIB within 90 calendar days of the date the investigation closed. The certificate affirms that GSA has made a suitability determination. OPM/NBIB does not use the certificate to indicate a favorable determination; rather, that GSA has reviewed the investigation and has made a determination. The Security Specialist prints out a certification from HR Links along with a copy of GSA Form 3665 and forwards it to CPC to be placed in the e-OPF.

(4) Reciprocity. Some Federal employees/applicants may have already been

investigated by another Federal agency. GSA uses these investigations whenever practicable to reduce the number of investigation requests, associated costs, and unnecessary delays. The following standards for use of these investigations apply:

(a) New forms are obtained and pre-employment checks completed.

(b) Any investigation conducted by, or for, another Federal agency on a Federal employee/applicant that is of the same or higher risk and scope as the one required is sufficient to meet the investigative requirements if the investigation was conducted within the past five years.

The investigation is requested and reviewed in conjunction with pre-employment checks to make a suitability decision for employment in accordance with the Adjudicative Criteria found in Appendix B. If the investigation is unavailable, a new, appropriate investigation must be completed.

4. Tier 1/Low Risk (Non-sensitive) positions.

a. Supervisor. The supervisor should have a copy of the position designation which indicates the risk level and the investigation required for the position.

b. OHRM. OHRM has the candidate complete the necessary forms, then reviews the forms for completeness, accuracy, and identifies any issues before submitting to the Personnel Security Branch for review. If any issues are identified by the Personnel Security Branch, the forms will be returned to OHRM for correction.

5. Tier 2/Moderate Risk and Tier 4/High Risk (Public Trust) positions. Processing for Tier 2 Moderate Risk and Tier 4 High Risk positions is similar to processing Low Risk positions. The major differences are:

a. Candidate. The candidate uses a different questionnaire (SF 85P).

b. Supervisor. The supervisor will initiate the action with the servicing OHRM when a current employee moves into a position that requires a higher position designation.

c. Personnel Security Branch. OMA has the authority to fund all GSA background investigations for the Agency. If the candidate has had the appropriate investigation in the past, the Personnel Security Branch will verify the certification.

d. Servicing OHRM.

(1) Arranges for all new candidates to complete the appropriate investigative forms as shown in Appendix G.

(2) Retrieves the investigative forms from the candidate and ensures the accuracy and completeness of all forms prior to submitting the completed package to the Personnel Security Branch.

(3) Coordinates the completion of the personnel investigation and favorable adjudication.

Note: Candidates with a prior favorably adjudicated investigation that meets or exceeds the current investigation requirements do not have to undergo a new investigation unless there has been a break in Federal service of more than two years, or the duties of the position are significantly different from the prior work.

e. Personnel Security Branch. This office reviews the forms for completeness and accuracy and forwards the package to OPM/NBIB for all investigations. OPM/NBIB completes advance fingerprint checks. When the Personnel Security Branch receives favorable fingerprint results, a notification is sent via e-mail to OHRM, IT Security, and OMA's HSPD-12 Branch. If the results are not favorable, the Personnel Security Branch may do further investigation or wait for OPM/NBIB to complete the background investigation before adjudicating the case. The Personnel Security Branch will notify the OHRM once adjudication is completed.

6. Reinvestigation. 5 CFR 731.106, Designation of public trust positions and investigative requirements, established a requirement to reinvestigate persons in positions of Public Trust (Tier 2R (Reinvestigation)/Moderate Risk and Tier 4R/High Risk) at least once every five years. The Personnel Security Branch will request the reinvestigation within four months of the anniversary of the previous investigation's completion date. Prior to submitting the request (or initiating the investigation locally), OHRM must ensure the individual still occupies a position of Public Trust. (See Appendix A for a detailed description of the Tiered investigation levels.)

CHAPTER 3

NATIONAL SECURITY

1. National security positions.

a. Positions whose duties require GSA employees to work with National Security Information (Top Secret, Secret, or Confidential), are national security positions. The Personnel Security Branch grants national security clearances to employees who need access to classified information.

b. GSA will only grant security clearances to employees in positions that meet the criteria for access to classified information.

c. All positions in GSA not designated as Non-Sensitive will be designated as Non Critical-Sensitive, Critical-Sensitive, or Special-Sensitive. As enumerated in 5 CFR Part 1400, all positions subject to investigation that could bring about an adverse effect on national security or require access to classified information must also receive a sensitivity designation of Tier 5/Special-Sensitive, Tier 5/Critical-Sensitive, or Tier 3/Noncritical-Sensitive. This designation is in addition to the risk level determination and may have an impact on the position's investigative requirements.

2. National security. All employees must be found to be suitable in order to work at GSA. In addition, persons whose duties require access to classified National Security Information must satisfy the requirements to hold a sensitive position in accordance with SEAD 4 and Executive Order 12968, as amended. The employee's position designation must indicate the national security level.

3. National security levels. The level and access determine whether or not the OHRM personnel may place the candidate into the position before the Personnel Security Branch grants the clearance. GSA uses the investigation to decide if employing the person is clearly consistent with the national security. The position's sensitivity level determines the relative seriousness with which adjudicators view issues developed in the investigation.

4. Security clearance. Eligibility for access to classified information, commonly known as a security clearance, is granted only to those for whom an appropriate background investigation has been completed. It must be determined that the individual's personal and professional history indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion and sound judgment. It must ensure freedom from conflicting allegiances and potential for coercion, and a willingness and ability to abide by regulations governing the use, handling, and protection of classified information. A determination of eligibility for access to such information is a discretionary security decision based on judgments by appropriately trained adjudicative personnel using the adjudicative guidelines (Appendix C). Eligibility will be granted only

where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States. Access to classified information will be terminated when an individual leaves GSA or no longer has a need for access.

5. Reciprocity.

a. In accordance with SEAD 7, if background investigations and national security eligibility adjudications meet the requirements for reciprocal acceptance, the following apply except as noted below in subparagraph b:

(1) A new Standard Form 86 (SF86), Questionnaire for National Security Positions, shall not be requested;

(2) The current background investigation, or the SF86 upon which it was based, will not be reviewed or re-adjudicated for national security purposes; and

(3) No new investigative checks will be initiated.

b. Agencies should initiate additional security processing if any of the following circumstances apply:

(1) When a background investigation has not been adjudicated, or does not meet the standard for the type of investigation required, the agency should review the investigative record and conduct the necessary investigative checks through an authorized investigative agency to ensure that the investigation is current and meets the standard for the type of investigation required. The agency should not duplicate investigative elements that are unlikely to change.

(2) If the agency requests updated security information from the last SF86 submission, and the covered individual indicates there has been a change to the information provided for the last background investigation, the agency should review the investigative record and conduct the necessary investigation in terms of the changed information.

6. Non-career Senior Executive Service (SES), Career SES and Critical-Sensitive Schedule C Candidates. GSA uses the pre-appointment procedures in Appendix F for all positions that require Top Secret national security clearances. These procedures do not apply to Schedule C candidates for public trust positions or for national security positions requiring **Secret** or **Confidential** national security clearances.

7. Responsibilities.

a. Personnel Security Branch. This office manages the National Security Program. It is the only organization in GSA that may request personnel investigations for national security positions and grant national security clearances.

b. Servicing OHRM. OHRM assists the Personnel Security Branch by requiring timely submission of investigative paperwork.

c. OMA Deputy Regional Director (DRD). The OMA DRD works closely with the Personnel Security Branch and will be notified when GSA employees are cleared for access to national security information. The OMA DRD will assist the Personnel Security Branch by conducting the initial, refresher and termination briefings for GSA employees assigned to their Regions. The OMA DRD will notify the Personnel Security Branch of any known issues regarding cleared GSA personnel.

8. How the national security program works.

a. Designating national security positions.

(1) All positions in GSA will be designated by OHRM's National Classification Center using the OPM Position Designation Automated Tool.

(2) The manager or supervisor must provide a justification for the security clearance on the GSA Position Risk Determination Survey.

(3) If the position is occupied when the position designation changes to national security, the employee must complete the investigative forms or be removed from the position. The employee will have 5 calendar days to complete the Electronic Questionnaires for Investigations Processing (e-QIP) application (background investigation). The Personnel Security Branch has 14 calendar days to request the investigation after the employee occupies the position.

b. Investigations to determine security fitness.

(1) Servicing OHRMs will submit the required forms, also known as the security packet to the Personnel Security Branch. The Personnel Security Branch is the only branch authorized to requests investigations for national security positions. OPM/NBIB conducts the investigation and returns all closed investigations to the Personnel Security Branch.

(2) The Personnel Security Branch receives investigations or other reports on a GSA employee in a national security position who may have engaged in disqualifying conduct. In such cases, the Personnel Security Branch must review the information, conduct any additional investigations necessary to resolve issues; and determine if the employee continues to be eligible for the national security position.

c. Security determinations. The Personnel Security Branch adjudicates personnel investigations to determine candidates' security fitness for sensitive positions. The Personnel Security Branch does not consider a case for adjudication until OPM/NBIB completes the investigation. The Personnel Security Branch adjudicates the results using the criteria in EO 12968, as amended. If the determination is favorable, the

Security Specialist grants or continues the clearance. (See Appendix C for guidance on making national security determinations.)

d. Briefings and Classified Information Nondisclosure Agreement. The Personnel Security Branch must ensure that each employee who has been granted a security clearance receives a briefing on security matters. The Standard Form 312 (SF 312) is the Classified Information Nondisclosure Agreement. A security briefing and a signed SF 312 must be completed before a person is granted access to classified material. The original or copy of the SF 312 must be sent to the Personnel Security Branch.

e. Due process. If security determinations are adjudicated unfavorably, the Security Specialist uses the due process provisions outlined herein. After the due process procedures are completed, the Personnel Security Branch can grant, revoke, deny the security clearance, or continue eligibility for a security clearance. (See Appendix I for more information about Due Process.)

9. Eligibility rules for national security positions. EO 12968, as amended, Section 2.1 places eligibility restrictions on national security positions in terms of having access to classified information. Those applicable restrictions are as follow:

a. The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

b. Eligibility for access to classified information shall not be requested or granted solely to permit entry to, or ease of movement within, controlled areas when the employee has no need for access and access to classified information may reasonably be prevented. Where circumstances indicate employees may be inadvertently exposed to classified information in the course of their duties, agencies are authorized to grant or deny, in their discretion, facility access approvals to such employees based on an appropriate level of investigation as determined by each agency.

c. Eligibility for access to classified information may be granted where there is a temporary need for access, such as one-time participation in a classified project, provided the investigative standards established under this order have been satisfied. In such cases, a fixed date or event for expiration shall be identified and access to classified information shall be limited to information related to the particular project or assignment.

d. Access to classified information shall be terminated when an employee no longer has a need for access.

10. Responsibilities.

a. Manager. The GSA management official plays an important role in the hiring process for national security positions.

(1) Action. The manager is responsible for informing OHRM that the position is a national security position.

(2) Special circumstances. In exceptional circumstances where official functions must be performed prior to the completion of the investigative and adjudication process, the Personnel Security Branch will follow its procedures to grant temporary eligibility for access to classified information to an employee while the initial investigation is underway. When such eligibility is granted, the initial investigation shall be expedited. If the Personnel Security Branch denies a security clearance to the employee, OHRM must remove the person from the national security position.

b. Servicing OHRM.

(1) Vacancy announcements for competitive and non-competitive personnel actions. OHRM prepares a vacancy announcement. The announcement must include one of the following statements:

(a) Special-sensitive position. This position is a special-sensitive national security position. To work in this position, you must undergo a Tier 5 background investigation and be able to obtain and maintain a Top Secret national security clearance with access to Sensitive Compartmented Information (SCI). The Personnel Security Branch must grant the clearance before GSA can hire the candidate. This requirement cannot be waived.

(b) Critical sensitive position. This position is a critical-sensitive national security position. To work in this position, you must undergo a Tier 5 background investigation and be able to obtain and maintain a Top Secret national security clearance.

(c) Non-critical sensitive position. This position is a non-critical sensitive national security position. To work in this position, you must undergo a Tier 3 or Tier 5 background investigation and be able to obtain and maintain a Secret or Confidential national security clearance.

(2) Security forms. Managers and OHRM coordinate to ensure that the candidates complete their security forms. The Personnel Security Branch reviews the forms for completeness and accuracy; and releases the security forms to OPM/NBIB for investigation. (See Appendix G for more information on forms).

11. Reinvestigations. 5 CFR 732.203 requires reinvestigations for all employees who hold national security clearances.

a. Top Secret security clearance. The Personnel Security Branch requests a Tier 5R be completed 4 years and 6 months after the last investigation for every employee in a special or critical-sensitive position with a Top Secret security clearance or Top Secret eligibility.

b. Secret security clearance. The Personnel Security Branch requests an investigation 9 years and 6 months after the previous investigation.

c. Personnel Security Branch. The HRLinks - Alert automated program notifies the Servicing OHRM, the employee, and Personnel Security Branch that it is time for a reinvestigation, and provides a due date for submission of the security forms. Upon receiving the forms, the Personnel Security Branch reviews them for completeness and accuracy, and releases the security forms to OPM/NBIB for the reinvestigation.

(1) The required documents must reach OPM/NBIB within 14 calendar days from the e-QIP certification date.

(2) OHRM is responsible for the following actions:

(a) Verify employee's employment status;

(b) Position Sensitivity/Risk level via Position Description (PD); and

(c) Submit required paperwork for all re-investigations.

d. Out-of-scope (overdue) clearances. If the re-investigative forms are not received by the anniversary date of the previous investigation, the automated program in HR Links sends a removal notice to the Personnel Security Branch e-mail address.

(1) The Personnel Security Branch will contact OHRM, the employee, and the employee's supervisor.

(2) OHRM will validate the position requirements and notify the Personnel Security Branch.

(3) The supervisor validates if the clearance is still needed.

(4) If the employee no longer needs the clearance, they are required to complete an SF-312, Non-Disclosure Agreement form immediately upon leaving the position that required access to classified information.

(5) In an exceptional circumstance in which an employee is unable to submit a periodic reinvestigation due to circumstances beyond their control, employee access to classified information will be maintained. In this case, the employee is responsible to submit the periodic reinvestigation as soon as possible. Such situations are addressed on a case-by-case basis.

CHAPTER 4

WAIVERS, TEMPORARY NATIONAL SECURITY CLEARANCES, AND TEMPORARY ASSIGNMENTS

1. General. The National Security interest dictates that GSA should not appoint persons to National Security positions until they have undergone personnel security investigations. Since GSA imposes no pre-appointment requirements for public trust positions, the issue of waivers does not arise concerning appointments to positions that are not national security positions. To meet special operational needs, the Personnel Security Branch may grant an interim **SECRET** security clearance for up to 180 calendar days.

2. Waivers. In an emergency, the Administrator, the Personnel Security Branch Officer, or designee may waive the pre-appointment investigation in the National Security interest. Only HSSOs or the Executive Resources Division (CPX), may request waivers.

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

b. If the position is designated as Tier 5/Critical Sensitive, the investigation should be completed before appointment; however, a waiver is permitted.

(1) OHRM may not appoint a non-GSA employee to a critical-sensitive position requiring Top Secret security clearance until the Personnel Security Branch has approved the waiver request. This prohibition also applies to GSA employees who have been on board less than one year in a Tier 1 (Non-sensitive) position.

(2) The HSSO or CPX may use Appendix H as a guide for preparing the waiver request to ensure that they have included all necessary information. An original waiver request must be submitted to the Personnel Security Branch along with the justification letter.

(3) Before approving the waiver, the Personnel Security Branch must request the Tier 5 investigation and have favorable results of the pre-employment checks listed below. The pre-employment checks include:

(a) Review of the SF-86; Questionnaire for National Security Positions;

(b) Review of the credit report;

(c) Review of the results of the fingerprint Special Agreement Check (SAC);

(d) Review of the Optional Form 306, Declaration for Federal Employment;

(e) Review of the position description;

(f) Verify investigative information available from OPM's Central Verification System (CVS)/Personnel Investigations Processing System (PIPS); and

(g) If the Personnel Security Branch finds any issues, then an interview with the candidate is required.

(4) The Personnel Security Branch does not routinely grant an interim National Security Clearance with the waiver; however, managers may request such a clearance as part of the waiver request. (Note: GSA does not grant "interim" Top Secret clearances; however, a Secret clearance may be requested.)

(5) The Personnel Security Branch sends the approved waiver to the requesting official who is responsible for coordinating with the servicing OHRM to bring the candidate into the position.

c. If the position is designated as Tier 3/Non-Critical Sensitive, no waiver is required.

3. Non-Critical Sensitive Position. Since GSA imposes no pre-appointment requirements for Non-Critical Sensitive Positions, the issue of waivers is not valid. If employees require temporary access while awaiting completion of the investigation, the managers and the Personnel Security Branch use paragraph 4b, below.

4. Temporary access to National Security Information. Based on a justified need and meeting the requirements of Section 3.3 of Executive Order 12968, as amended, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, for a specific time period (up to 180 calendar days), where official functions must be performed prior to completion of the investigation and adjudication process. Before the Personnel Security Branch grants the temporary clearances, the employees must receive a national security briefing and sign the SF-312, Classified Information Nondisclosure Agreement. After favorable review of a SF-86 and credit check, the Personnel Security Branch provides the requester and OMA DRD notification of the determination to grant limited access.

a. Requesting temporary access. Only HSSOs and CPX may request temporary clearances. In all cases, the officials must include in their requests (see Appendix H for GSA's Waiver Request template):

(1) A justification for the temporary access.

(2) The classification categories of information the employee will access to perform lawful and authorized functions are as follows:

(a) Military plans, weapons systems, or operations;

(b) Foreign government information;

(c) Intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) Foreign relations or foreign activities of the United States, including confidential sources;

(e) Scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities;

(g) Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security; or

(h) The development, production, or use of weapons of mass destruction.

b. Temporary assignments. If the employee has a temporary assignment that requires access to classified information, the managers must contact the Personnel Security Branch for a temporary security clearance. Managers are responsible for preventing employees who have not been cleared by the Personnel Security Branch from accessing classified information.

CHAPTER 5

MISCELLANEOUS

1. Special clearances. GSA employees who work with or at other Federal agencies may need special clearances or access. All organizations or agencies that require a special clearance or access must contact the Personnel Security Branch for information about the procedures. The special clearance or access is controlled by the agency, and GSA has no recourse if an agency denies the clearance or access to GSA employees. Below are some agencies that issue special clearances or access:

a. Department of Energy and the Nuclear Regulatory Commission (Q and L clearances);

b. Department of Defense (North Atlantic Treaty Organization clearances).

2. Sensitive Compartmented Information (SCI). If the position requires access to SCI, the PD must indicate that a Top Secret clearance and SCI access is required. If the original PD does not indicate that the position requires SCI, an SCI justification will need to be sent to the Personnel Security Branch explaining why the position requires access to SCI. Requests for SCI should only be submitted on individuals who hold a Top Secret clearance. The Central Intelligence Agency is responsible for granting GSA employees SCI access.

3. Official visits by foreign nationals. GSA officials must contact the Personnel Security Branch if foreign nationals are scheduled to visit sites that store classified information. The GSA officials must provide the following information:

a. Purpose of the visit;

b. Each visitor’s name, date and place of birth, itineraries, contacts, and sponsors;

c. Arrangements for monitoring the visitors while they are on GSA property;

d. Comments on whether the visit is consistent with national policy; and

e. Comments on whether GSA will reciprocate with visits to the foreign country.

4. Foreign travel. GSA employees with a security clearance (e.g., Secret, Top Secret), are required to provide notice to the OMA Threat Management Office (TMO) of all foreign travel, conducted for either official or personal purposes, at least 2 weeks in advance of travel. Foreign travel is defined as travel outside the United States and its territories. Such employees may be required to receive a travel briefing prior to foreign travel and may be subject to a security debrief upon completion of foreign travel. GSA employees without a security clearance are encouraged but not required to notify the OMA TMO of all foreign travel, conducted for either official or personal purposes. Such

employees may receive travel briefings prior to foreign travel and may be asked to participate in a security debrief upon completion of foreign travel. GSA employees are prohibited from taking Government-furnished electronic devices (including laptops, tablets, phones or other equipment) on foreign travel unless cleared by the Personnel Security Branch and GSA IT.

5. Security services for Commissions, Boards or other entities which GSA supports. GSA provides administrative support services when directed by law or when requested. As part of this support, the Commissions and Boards Services' (CABS) Business and Administrative Management Division, and the Personnel Security Branch assist the organizations with their suitability and security programs under the requirements of 5 CFR Parts 731, 732, and 736; EO 13764; EO 12968, as amended; and, HSPD-12.

a. The CABS Servicing Human Resources Office (SHRO) provides guidance to the organizations in designating their positions under public trust and national security. If they use GSA personnel and security services, the organizations are responsible for notifying CABS SHRO and the Personnel Security Branch about the designations. GSA must have the designations before requesting personnel investigations.

b. CABS SHRO is responsible for providing the appropriate investigative forms to the Personnel Security Branch. The Personnel Security Branch requests all investigations for CABS personnel.

c. The Personnel Security Branch reviews and adjudicates all reports of investigations including derogatory reports for suitability or security.

6. Fingerprinting/SAC.

a. Every effort should be made to have applicants (new hires, affiliates, etc.) fingerprinted prior to the applicant's entrance on duty (EOD).

b. Fingerprint SACs must be submitted to OPM electronically. If this is not possible, fingerprints will be captured within 5 calendar days of EOD. In certain instances where the applicant is overseas or not close to an enrollment station SF-87, Fingerprint Cards may be used and submitted to the Personnel Security Branch for processing.

7. Incoming visitors and detailees requiring access to classified GSA information and systems. Non-GSA employees must be certified to access classified GSA information and systems. In order to do so, the incoming visitor's or detailee's Personnel Security Branch (or equivalent) must pass their security clearances and/or background investigation information via a Visit Authorization Request to GSA Personnel Security Branch by fax to (202) 208-4296 or by email gsa.securityoffice@gsa.gov.

8. Security files and investigation records.

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

b. Security files (if not electronic) will be stored in locked cabinets and in a secured room. All documentation must be maintained for at least 1 year and not longer than 5 years after the employee relationship ends, but longer retention is authorized if required for business use.

c. The security files can be stored electronically instead of the traditional hard copy folders. The electronic security files must contain all the required information from the Report of Investigation (ROI). The security files will contain (as appropriate):

(1) Case Closing Transmittal;

(2) Certificate of Investigation;

(3) Any derogatory information developed or received in the course of the investigation;

(4) Security questionnaire;

(5) Suitability worksheet; and

(6) SF 312, Classified Information Nondisclosure Agreement.

9. Reporting requirement for covered employees. SEAD 3 establishes reporting requirements for all covered individuals who have access to classified information or who hold a sensitive position. Covered individuals have a special and continuing security obligation and responsibility for recognizing, avoiding, and reporting personal behaviors of a potential security, counterintelligence, and/or insider threat concern. Individuals must alert their Security Officer should they become personally involved with or aware of certain activities of other covered individuals that may be of potential security, counterintelligence, and/or insider threat concern. (Reference Appendix E for additional information).

CHAPTER 6

SECURITY AWARENESS, EDUCATION AND TRAINING

1. General.

a. EO 13526, as amended, Classified National Security Information, mandates that every person who receives a favorable determination of eligibility for access receive training on the proper safeguarding of classified information and the sanctions imposed on those who fail to appropriately protect such information. Additionally, it authorizes the Director of the Information Security Oversight Office, under the direction of the Archivist and in consultation with the National Security Advisor, to establish standards for GSA security education and training programs. The EO also lays out the requirement for the GSA Administrator to designate a senior agency official (in this instance, the OMA Associate Administrator) to establish and maintain these programs.

b. EO 12968, as amended, Access to Classified Information, requires that the GSA Administrator educate employees about their individual responsibilities for handling classified information and inform them about issues that may affect their eligibility for access to classified information. Security education is any activity undertaken to ensure that people have the skills, knowledge, and information to enable quality performance of security functions and responsibilities, understand security program policies and requirements, and maintain continued awareness of security requirements and intelligence threats. An effective security education and training program enables cleared personnel to protect classified national security information and meet their security responsibilities.

2. Initial security briefing. In order for cleared personnel to receive access to classified information; they must first receive an initial security briefing and then execute SF-312, the Classified Information Nondisclosure Agreement. The SF-312 briefing may either be included in the initial briefing or upon the individual's receiving a favorable determination of eligibility for access.

a. After the briefing, personnel who sign and execute the SF-312 are granted access to classified information at their authorized access level and on a need-to-know basis. Executed SF-312s are then forwarded to the Personnel Security Branch and entered into the system of record. If an individual refuses to execute the SF-312, action shall be initiated to deny or revoke the individual's security clearance.

b. All initial briefings must cover basic security roles and responsibilities, provide an overview of the classification system, and discuss the penalties for disclosing classified information to unauthorized individuals. GSA requires training for all individuals cleared for access to classified information. This training must include:

(1) Security requirements specific to their particular job;

(2) Techniques employed by foreign intelligence activities to obtain classified information and employee responsibility for reporting those attempts;

(3) The prohibition against disclosure of classified information to unauthorized individuals;

(4) The responsibility for continuous evaluation of one's own and others' security activities; and

(5) The penalties that may be imposed for security violations.

3. Periodic refresher. GSA mandates that all cleared personnel attend refresher training annually. Refresher training does the following:

a. Reinforces the information covered in the initial briefing and in any specialized training, including security policies, principles and procedures, and penalties for engaging in espionage and other security violations;

b. Addresses new threats and foreign intelligence techniques and discuss any changes in security regulations;

c. Addresses any issues or concerns identified during security inspections and self-inspections; and

d. Tailors the content and format of refresher briefings to meet the needs of the audience of experienced personnel. Refresher training is accomplished via GSA Online University.

e. Maintains a record of completion of refresher training sessions allowing the Personnel Security Branch to keep track of all GSA employees who have received the training.

4. Debriefing.

a. GSA mandates debriefings when an employee terminates employment or is discharged, and when an employee's access to classified information is terminated, suspended, revoked, or no longer required by the position. The debriefing should cover:

(1) The individual's continued responsibility to protect classified information;

(2) The continuing requirement for the individual to report attempts by unauthorized individuals to gain access to classified information;

(3) The prohibition against retaining classified materials; and

(4) The civil and criminal penalties for violating security regulations and disclosing classified information.

b. The debriefing is followed by the employee signing the SF-312. If an employee is not present or refuses to receive a security debriefing when classified access is terminated, then the fact and reasons for the person's absence and or refusal become a matter of record and must be reported immediately to Personnel Security Branch. If this occurs (i.e., an employee leaves without being properly debriefed by security personnel), the statement "administratively debriefed" will be typed in the signature block where the employee should have signed to terminate the employee's access.

APPENDIX A. NATIONAL SECURITY POSITIONS - SENSITIVITY LEVELS AND DESIGNATION REQUIREMENTS

[In accordance with 5 CFR 732.201(b), investigative requirements for each sensitivity level are provided for by OPM.]

<table>
<tr><th colspan="2">National Security Positions (see 5 CFR § 1400.201)</th></tr>
<tr><th>Sensitivity Level</th><th>Designation Requirements</th></tr>
<tr><td rowspan="2">(1) Noncritical-Sensitive positions are national security positions which have the potential to cause significant or serious damage to the national security, including but not limited to:</td><td>(i) Positions requiring eligibility for access to Secret, Confidential, or “L” classified information; or</td></tr>
<tr><td>(ii) Positions not requiring eligibility for access to classified information, but having the potential to cause significant or serious damage to the national security.</td></tr>
<tr><td>(2) Critical-Sensitive positions are national security positions which have the potential to cause exceptionally grave damage to the national security, including but not limited to:</td><td rowspan="2">(i) Positions requiring eligibility for access to Top Secret or “Q” classified information;

(ii) Positions not requiring eligibility for access to classified information, but having the potential to cause exceptionally grave damage to the national security;

(iii) Positions involving development or approval of war plans, major or special military operations, or critical and extremely important items of war;

(iv) National security policy-making or policy-determining positions;

(v) Positions with investigative duties, including handling of completed counterintelligence or background investigations, the nature of which have the potential to cause exceptionally grave damage to the national security;

(vi) Positions involving national security adjudicative determinations or granting of personnel security clearance eligibility;

(vii) Positions involving duty on personnel security boards;

(viii) Senior management positions in key</td></tr>
<tr><td></td></tr>
</table>

	programs, the compromise of which could result in exceptionally grave damage to the national security; (ix) Positions having direct involvement with diplomatic relations and negotiations; (x) Positions involving independent responsibility for planning or approving continuity of Government operations; (xi) Positions involving major and immediate responsibility for, and the ability to act independently without detection to compromise or exploit, the protection, control, and safety of the nation's borders and ports or immigration or customs control or policies, where there is a potential to cause exceptionally grave damage to the national security; (xii) Positions involving major and immediate responsibility for, and the ability to act independently without detection to compromise or exploit, the design, installation, operation, or maintenance of critical infrastructure systems or programs; (xiii) Positions in which the occupants have the ability to independently damage public health and safety with devastating results; (xiv) Positions in which the occupants have the ability to independently compromise or exploit biological select agents or toxins, chemical agents, nuclear materials, or other hazardous materials; (xv) Positions in which the occupants have the ability to independently compromise or exploit the nation's nuclear or chemical weapons designs or systems; (xvi) Positions in which the occupants obligate, expend, collect or control revenue, funds or items with monetary value in excess of $50 million, or procure or secure funding for goods and/or services with monetary value in excess of $50 million annually, with the potential for

	exceptionally grave damage to the national security; (xvii) Positions in which the occupants have unlimited access to and control over unclassified information, which may include private, proprietary or other controlled unclassified information, but only where the unauthorized disclosure of that information could cause exceptionally grave damage to the national security; (xviii) Positions in which the occupants have direct, unrestricted control over supplies of arms, ammunition, or explosives or control over any weapons of mass destruction; (xix) Positions in which the occupants have unlimited access to or control of access to designated restricted areas or restricted facilities that maintain national security information classified at the Top Secret or "Q" level; (xx) Positions working with significant life-critical/mission-critical systems, such that compromise or exploitation of those systems would cause exceptionally grave damage to essential Government operations or national infrastructure; or (xxi) Positions in which the occupants conduct internal and/or external investigation, inquiries, or audits related to the functions described in paragraphs (a)(2)(i) through (xx) of this section, where the occupant's neglect, action, or inaction could cause exceptionally grave damage to the national security.
(3) Special-Sensitive positions are those national security positions which have the potential to cause inestimable damage to the national security, including but not limited to:	(i) Positions requiring eligibility for access to Sensitive Compartmented Information (SCI); or (ii) Positions requiring eligibility for access to any other intelligence-related Special Sensitive information; or (iii) Positions requiring involvement in Top

	Secret Special Access Programs (SAP); or iv) Positions which the agency head determines must be designated higher than Critical-Sensitive consistent with Executive order.

Non-Sensitive Public Trust Positions	
Sensitivity Level	Designation Requirements
Public Trust positions. Positions at the **high** or **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.
Low Risk Non-sensitive	All other positions not designated as Sensitive.

APPENDIX B. CRITERIA FOR MAKING SUITABILITY DETERMINATIONS

The standard for a suitability action defined in 5 CFR 731.203 and taken against an applicant, appointee, or employee is that the action will protect the integrity or promote the efficiency of the service.

In determining whether a person is suitable for Federal employment, only the following factors will be considered a basis for finding a person unsuitable and taking a suitability action (5 CFR 731.202):

(1) Misconduct or negligence in employment;

(2) Criminal or dishonest conduct;

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

(4) Refusal to furnish testimony as required by § 5.4 of this chapter;

(5) Alcohol abuse, without evidence of substantial rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of the applicant or appointee or others;

(6) Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation;

(7) Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; and

(8) Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

As outlined in 5 CFR 731.202(c), GSA Personnel Security must also consider any of the following additional considerations to the extent they are deemed pertinent to the individual case:

(1) The nature of the position for which the person is applying or in which the person is employed;

(2) The nature and seriousness of the conduct;

(3) The circumstances surrounding the conduct;

(4) The recency of the conduct;

(5) The age of the person involved at the time of the conduct;

(6) Contributing societal conditions; and

(7) The absence or presence of rehabilitation or efforts toward rehabilitation.

Reciprocity. An agency cannot make a new determination under this section for a person who has already been determined suitable or fit based on character or conduct unless a new investigation is required under 5 CFR 731.104 or 5 CFR 731.106, or no new investigation is required but the investigative record on file for the person shows conduct that is incompatible with the core duties of the relevant covered position.

APPENDIX C. MAKING NATIONAL SECURITY DETERMINATIONS

Direct Source: Security Executive Agent Directive 4 - National Security Adjudicative Guidelines, Effective June 8, 2017 -- https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf

1. National Security Adjudicative Guidelines.

a. The following National Security Adjudicative Guidelines ("guidelines") are established as the single common criteria for all U.S. Government civilian and military personnel, consultants, contractors, licensees, certificate holders or grantees, and their employees,…and other individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position, to include access to sensitive compartmented information, restricted data, and controlled or special access program information (hereafter referred to as "national security eligibility"). These guidelines shall be used by all Executive Branch Agencies when rendering any final national security eligibility determination.

b. National security eligibility determinations take into account a person's stability, trustworthiness, reliability, discretion, character, honesty, and judgment. Individuals must be unquestionably loyal to the United States. No amount of oversight or security procedures can replace the self-discipline and integrity of an individual entrusted to protect the nation's secrets or occupying a sensitive position. When a person's life history shows evidence of unreliability or untrustworthiness, questions arise as to whether the individual can be relied upon and trusted to exercise the responsibility necessary for working in an environment where protecting the national security is paramount.

c. The U.S. Government does not discriminate on the basis of race, color, religion, sex, national origin, disability, or sexual orientation in making a national security eligibility determination. No negative inference concerning eligibility under these guidelines may be raised solely on the basis of mental health counseling. No adverse action concerning these guidelines may be taken solely on the basis of polygraph examination technical calls in the absence of adjudicatively significant information.

d. In accordance with EO 12968, as amended, eligibility for covered individuals shall be granted only when facts and circumstances indicate that eligibility is clearly consistent with the national security interests of the United States, and any doubt shall be resolved in favor of national security.

2. The Adjudicative Process.

a. The adjudicative process is an examination of a sufficient period and a careful weighing of a number of variables of an individual's life to make an affirmative determination that the individual is an acceptable security risk. This is known as the

whole-person concept. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a national security eligibility determination.

b. Each case must be judged on its own merits, and the final determination remains the responsibility of the authorized adjudicative agency. Any doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security.

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

(1) GUIDELINE A: Allegiance to the United States

(2) GUIDELINE B: Foreign Influence

(3) GUIDELINE C: Foreign Preference

(4) GUIDELINE D: Sexual Behavior

(5) GUIDELINE E: Personal Conduct

(6) GUIDELINE F: Financial Considerations

(7) GUIDELINE G: Alcohol Consumption

(8) GUIDELINE H: Drug Involvement and Substance Misuse

(9) GUIDELINE I: Psychological Conditions

(10) GUIDELINE J: Criminal Conduct

(11) GUIDELINE K: Handling Protected Information

(12) GUIDELINE L: Outside Activities

(13) GUIDELINE M: Use of Information Technology

d. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

(1) The nature, extent, and seriousness of the conduct;

(2) The circumstances surrounding the conduct, to include knowledgeable participation;

(3) The frequency and recency of the conduct;

(4) The individual's age and maturity at the time of the conduct;

(5) The extent to which participation is voluntary;

(6) The presence or absence of rehabilitation and other permanent behavioral changes;

(7) The motivation for the conduct;

(8) The potential for pressure, coercion, exploitation, or duress; and

(9) The likelihood of continuation or recurrence.

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

f. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator will consider whether the person:

(1) Voluntarily reported the information;

(2) Was truthful and complete in responding to questions;

(3) Sought assistance and followed professional guidance, where appropriate;

(4) Resolved or appears likely to favorably resolve the security concern;

(5) Has demonstrated positive changes in behavior and employment; and

(6) Should have his or her access temporarily suspended pending final adjudication of the information.

g. If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

APPENDIX D. PASSING VISIT AUTHORIZATION LETTER/REQUEST

Passing Visit Authorization Letter/Request
(https://www.gsa.gov/forms-library/passing-visit-authorization-letterrequest)

PASSING VISIT AUTHORIZATION LETTER/REQUEST

(The Security Branch requires 48 hours prior to visit.)

Request to pass Collateral Clearance: E-Mail gsa.securityoffice@gsa.gov or Fax to (202) 219-0572

Request to pass SCI Accesses: E-Mail specialsecurityprograms@gsa.gov or (Fax) to (202) 219-3254

Name of Requestor: GSA Organization:

Date of Request: Requestor's Phone Number:

Name of Supervisor Authorizing Action:

Supervisor's Signature:

Please complete the information below in its entirety.
Failure to complete all information may result in processing delays.

Name of Individual who need VAL/VAR passed:

E-Mail Address: SSN (Last 4 Digits):

Date of Birth (DOB): Place of Birth (POB):

Visiting Agency:

Address:

City: State: ZIP Code:

Dates of Visit: From: To:

Purpose of Visit:

Clearance Level Required *(if applicable)*: ☐ Secret ☐ Top Secret ☐ TS/SCI

Visiting Agency POC:

First Name: Last Name:

Visiting Agency Phone Number:

Visiting Agency Security Office:

Visiting Agency Security Office Phone Number:

Visiting Agency Security Office Fax Number:

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires Federal agencies inform individuals at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN is needed to keep records accurate because other people many have the same name and birth date. Your SSN will be used to identify you precisely when it is necessary to certify that you have access as indicated above. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such clearance verifications and passing.

GENERAL SERVICES ADMINISTRATION GSA 6102 10/2016

APPENDIX E. REPORTING REQUIREMENTS FOR PERSONNEL WITH ACCESS TO CLASSIFIED INFORMATION OR WHO HOLD A SENSITIVE POSITION

[These requirements became effective under Security Executive Agent Directive (SEAD) 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position, June 12, 2017. The following language is contained in SEAD 3. The full text of SEAD 3 is available at https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf

F. REPORTABLE ACTIVITIES FOR ALL COVERED INDIVIDUALS:

1. Foreign Travel:

a. Heads of agencies or designees shall determine requirements for reporting foreign travel as part of a covered individual's official duties.

b. Unofficial Foreign Travel:

(1) Covered individuals shall submit an itinerary for unofficial foreign travel to their agency head or designee and, except as noted in the subparagraphs below, must receive approval prior to the foreign travel. Unanticipated border crossings into any foreign country not included in the traveler's approved itinerary, regardless of duration, are discouraged. All deviations from approved travel itineraries shall be reported within five business days of return.

(a) Travel to Puerto Rico, Guam, or other U.S. possessions and territories is not considered foreign travel and need not be reported.

(b) Unplanned day trips to Canada or Mexico shall be reported upon return. Reporting shall be within five business days.

(c) When required by the agency head or designee, covered individuals shall, prior to travel, receive a defensive security and counterintelligence briefing.

(d) While emergency circumstances may preclude full compliance with pre-travel reporting requirements, the covered individual, at a minimum, shall verbally advise their supervisor/management chain of the emergency foreign travel with all pertinent specifics and, preferably, a security representative, prior to departure. In any event, full reporting shall be accomplished within five business days of return.

(e) Consistent with national security, heads of agencies or designees may identify, for covered individuals under their purview, conditions under which prior reporting and approval of unofficial travel is not required, such as, agencies with an overseas presence that may require less specific reporting as opposed to every

instance, e.g. travelled to x country y times last month, travel weekly/monthly to x country, travel to x country y times per year, etc.

(2) Heads of agencies or designees may disapprove an unofficial foreign travel request when it is determined that such travel presents an unacceptable risk and the physical safety and security of covered individuals or classified information cannot be reasonably ensured. Failure to comply with such disapproval may result in administrative action that includes, but is not limited to, revocation of national security eligibility.

2. Foreign Contacts:

a. Heads of agencies or designees shall determine requirements for reporting contact with a foreign national as part of a covered individual's official duties.

b. Unofficial Contacts:

(1) Unofficial contact with a known or suspected foreign intelligence entity.

(2) Continuing association with known foreign nationals that involve bonds of affection, personal obligation, or intimate contact; or any contact with a foreign national that involves the exchange of personal information. This reporting requirement is based on the nature of the relationship regardless of how or where the foreign national contact was made or how the relationship is maintained (i.e. via personal contact, telephonic, postal system, Internet, etc.). The reporting of limited or casual public contact with foreign nationals is not required absent any other reporting requirement in this directive. Following initial reporting, updates regarding continuing unofficial association with known foreign nationals shall occur only if and when there is a significant change in the nature of the contact. Heads of agencies or designees may provide specific guidance and examples of updated reporting situations.

3. Reportable Actions by Others: To ensure the protection of classified information or other information specifically prohibited by law from disclosure, covered individuals shall alert agency heads or designees to the following reportable activities of other covered individuals that may be of potential security or counterintelligence (CI) concern:

a. An unwillingness to comply with rules and regulations or to cooperate with security requirements.

b. Unexplained affluence or excessive indebtedness.

c. Alcohol abuse.

d. Illegal use or misuse of drugs or drug activity.

e. Apparent or suspected mental health issues where there is reason to believe it may impact the covered individual's ability to protect classified information or other information specifically prohibited by law from disclosure.

f. Criminal conduct.

g. Any activity that raises doubts as to whether another covered individual's continued national security eligibility is clearly consistent with the interests of national security.

h. Misuse of U.S. Government property or information systems.

4. Covered individuals who have been identified by their respective agency head in accordance with EO 12968, as amended, Section 1.3. (a) shall file a financial disclosure report, as appropriate.

G. REPORTABLE ACTIVITIES FOR INDIVIDUALS WITH ACCESS TO SECRET AND CONFIDENTIAL INFORMATION, "L" ACCESS, OR HOLDING A NON-CRITICAL SENSITIVE POSITION: In addition to the reporting requirements in Section F, individuals with access to Secret and Confidential information, "L" access, or holding a Non-Critical sensitive position shall also report:

1. Foreign Activities:

a. Application for and receipt of foreign citizenship.

b. Application for, possession, or use of a foreign passport or identity card for travel.

2. Other Reportable Activities:

a. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.

b. Media contacts, other than for official purposes, where the media seeks access to classified information or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the covered individual need not be reported.

c. Arrests.

d. Bankruptcy or over 120 days delinquent on any debt.

e. Alcohol-and drug-related treatment.

H. REPORTABLE ACTIVITIES FOR INDIVIDUALS WITH ACCESS TO TOP SECRET INFORMATION, "Q" ACCESS, OR HOLDING A CRITICAL OR SPECIAL SENSITIVE POSITION: In addition to the reporting requirements in Section F, individuals with access to Top Secret information, "Q" access, or holding a Critical or Special sensitive position shall also report:

1. Foreign Activities:

   a. Direct involvement in foreign business.

   b. Foreign bank accounts.

   c. Ownership of foreign property.

   d. Application for and receipt of foreign citizenship.

   e. Application for, possession, or use of a foreign passport or identity card for travel.

   f. Voting in a foreign election.

   g. Adoption of non-U.S. citizen children.

2. Other Reportable Activities:

   a. Attempted elicitation, exploitation, blackmail, coercion, or enticement to obtain classified information or other information specifically prohibited by law from disclosure regardless of means.

   b. Media contacts where the media seeks access to classified information or other information specifically prohibited by law from disclosure, whether or not the contact results in an unauthorized disclosure. Media contacts related to the fulfillment of official duties of the position held by the covered individual need not be reported.

   c. Arrests.

   d. Financial Anomalies: Including, but not limited to, bankruptcy; garnishment; over 120 days delinquent on any debt; and any unusual infusion of assets of $10,000 or greater such as an inheritance, winnings, or similar financial gain.

   e. Foreign National Roommate(s): Any foreign national(s) who co-occupies a residence for a period of more than 30 calendar days.

   f. Cohabitant(s).

   g. Marriage.

   h. Alcohol- and drug-related treatment.

APPENDIX F. PERSONNEL SECURITY POLICY FOR NON-CAREER SES, CAREER SES, AND SCHEDULE C EMPLOYEES WITH TOP SECRET SECURITY CLEARANCES

1. Applicability. The Administrator, CPX, and the Personnel Security Branch use these procedures to determine the suitability and security fitness of persons assigned to non-career SES, career SES, and to Schedule C positions requiring Top Secret security clearances.

2. Exception. GSA does not use these procedures if the candidate is:

a. A Federal employee who has been investigated and adjudicated for a Top Secret security clearance within the past five years;

b. A GSA employee for at least one year; or

c. Currently certified by GSA for any national security or public trust position.

3. Check ahead. To speed processing, CPX may request a check ahead to reduce the time for processing waivers or expedited appointments. This procedure permits the Personnel Security Branch to begin advance checks while the candidate completes the security forms.

4. Procedures before CPX requests a waiver.

a. After tentatively selecting a candidate, CPX reviews the employment application for any potentially disqualifying suitability issues and forwards the security package to the Personnel Security Branch for a fast track. CPX brings to the attention of the Personnel Security Branch any potential issues in the application.

b. The Personnel Security Branch reviews any potentially disqualifying suitability issues, using appendix B. If the Personnel Security Branch does not find any issues, then the Personnel Security Branch begins the advance checks. CPX obtains the waiver request and the security forms then provides all the necessary information to the Personnel Security Branch.

c. If the Personnel Security Branch finds issues, it forwards the information to the Administrator or designee through the Personnel Security Branch for review on whether to continue the appointment process.

d. CPX may not appoint the candidate until the Personnel Security Branch or the Personnel Security Branch approves the waiver.

5. Action by the Personnel Security Branch after receiving the investigative forms.

a. The Personnel Security Branch thoroughly reviews the forms for completeness and accuracy. The Personnel Security Branch ensures the forms' integrity by requiring any changes or alterations to be initialed and dated by the person making the changes.

b. The Personnel Security Branch requests an expedited Tier 5 investigation (with advance NAC (National Agency Check) and credit report service) and begins the advance checks if it has not already started them.

c. If the Personnel Security Branch needs to interview the candidate, the office may contact the person directly or through CPX. During the interview, the Personnel Security Branch reviews the investigative forms with the candidate to ensure proper completion of the forms, and to fully elaborate on any suitability or security issues.

d. CPX and Personnel Security Branch will document the collective acquisition, review, and evaluation of all candidates.

6. Waiver approval.

a. After favorably adjudicating issues raised in the pre-appointment checks, the Personnel Security Branch may process the waiver for approval upon receipt of the advance NAC and credit report.

b. Only the Administrator, the Personnel Security Branch, or designee may approve the waiver.

c. After waiver approval, the Personnel Security Branch notifies CPX, who establishes the entrance on duty date. The Personnel Security Branch sends the original of the approved waiver to CPX for filing on the permanent side of the candidate's e-OPF.

7. Accountability of the Personnel Security Branch.

a. OPM provides investigative reports pending completion of its Tier 5 investigation.

(1) If OPM identifies no issues after their initial review, the investigation will be scheduled. The Personnel Security Branch retains the advance NAC reports in the security folder awaiting completion of the investigation.

(2) If OPM identifies issues and requires additional information, the Personnel Security Branch will review and contact the candidate and notify CPX.

(a) The Personnel Security Branch adjudicates all reports of investigations including derogatory reports for suitability or security.

(b) The Personnel Security Branch retains all other cases awaiting OPM's completion of the investigation.

b. Case closing.

(1) The Personnel Security Branch documents on the Security Specialist Worksheet the basis or rationale for granting clearances in those cases with potentially disqualifying suitability or security issues.

(2) The Personnel Security Branch keeps all cases when an unsuitable determination was made.

(a) The case file must contain all of the forms obtained or used by CPX and the Personnel Security Branch, except the SF 87.

(b) The file must also contain all pre-appointment checks, due process, and investigative reports pertaining to the case.

(3) The Personnel Security Branch completes Form 79A, Report of Agency Adjudicative Action on OPM Personnel Investigations and a copy is kept for all determinations.

APPENDIX G.
FORMS USED FOR PUBLIC TRUST AND NATIONAL SECURITY INVESTIGATION SUBMISSION

Investigation Forms for Non-Sensitive Positions (Tier 1)
1. SF 85, Questionnaire for Non-Sensitive Positions (eQIP)
2. SF 87, Fingerprint Chart and/or MSO (Electronic Fingerprints)
3. Resume (New Candidates Only)
4. Optional Form (OF) 306, Declaration for Federal Employment

Investigation Forms for Non-Sensitive Public Trust Positions (Tier 2 and Tier 4)
1. SF 85P, Questionnaire for Public Trust Positions (eQIP)
2. SF 87, Fingerprint Chart and/or MSO (Electronic Fingerprints)
3. Resume (New Candidates Only)
4. Optional Form (OF) 306, Declaration for Federal Employment
5. GSA Form 3665, Authorization to Obtain Credit Report
6. Additional Questions for Moderate Risk Positions - Branching

Investigation Forms for National Security Positions (Tier 3 and Tier 5)
1. SF 86, Questionnaire for National Security Positions (eQIP)
2. SF 87, Fingerprint Chart and/or MSO (Electronic Fingerprints)
3. Resume (New Candidates Only)
4. Optional Form (OF) 306, Declaration for Federal Employment
5. GSA Form 3665, Authorization to Obtain Credit Report
6. Justification
7. Waiver (if applicable)

APPENDIX H. WAIVER REQUEST FORM FOR BACKGROUND INVESTIGATION

MEMORANDUM FOR: Director, GSA Personnel Security Branch

FROM: <HSSO or CPX>

SUBJECT: Request for Waiver of Pre-appointment Investigation Requirement

Pursuant to 5 CFR 732.202, (insert office name) requests a waiver of the pre-appointment investigation for (name of applicant). This employee has been (appointed or assigned) to the position of (title).

A waiver of pre-appointment investigative requirements is being requested for emergency reasons and such action is necessary in the national security interest. (Specify urgency). If approved, I will ensure that the individual will not have access to any classified national security information prior to the granting of a national security clearance.

To request temporary access: (Name of candidate) requires temporary access to National Security Information at the SECRET level because (give justification). The particular categories that the candidate will access are (identify the categories). Categories can be found in Chapter 4, subparagraph 4.a.(2).

Approve: _____ Date:_____

Disapprove: _____ Date:_____

APPENDIX I. DUE PROCESS

1. General. When the Personnel Security Branch proposes to deny, suspend, or revoke a person's national security clearance or eligibility for a security clearance, the agency gives the person the opportunity to address the issues leading to the denial, suspension or revocation. This is called Due Process. The Personnel Security Branch oversees the due process procedures and is responsible for ensuring its fair application. This appendix applies only to actions involving national security clearances or eligibility.

2. Denying a national security clearance. When the request for a security clearance or eligibility is denied, the Personnel Security Branch sends a letter of intent to the person.

3. Notice of Proposed Action (NOPA). A letter sent to the applicant/employee with issues that were not mitigated during the adjudication of their investigation. This notice will include the specific issues, the amount of time to respond, and the address where the reply should be sent.

a. The letter will specify the reasons for proposing to deny the clearance or eligibility, based on the information in the investigation.

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

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

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

e. The Personnel Security Branch makes the final decision after reviewing all the information and sends a letter to the person. If an unfavorable decision is rendered, the Personnel Security Branch informs the person of the right to file a written appeal to the Personnel Security Specialist within 30 calendar days.

f. The subject will have the opportunity to appeal in writing to a high level panel, appointed by OMA Associate Administrator or designee which must comprise at least three members, two of whom must be selected from outside the security field. The decision of the appeals panel must be in writing, and will be final, except where the

Administrator or designee personally exercises the appeal authority based upon recommendations from the appeals panel. In such cases, the decision of the Administrator or designee will be final.

3. Suspending a national security clearance or eligibility. If the Personnel Security Branch receives information falling under the guidelines in Appendix C, the office reviews the information for security significance and completeness. If the office believes further investigation is necessary, the office may suspend the person's clearance and propose to revoke it. In such a case, the rest of this section does not apply.

a. The Personnel Security Branch arranges for further investigation to confirm or disprove the allegations. While the investigation is pending, the office may continue the employee's clearance or administratively suspend the clearance until making a decision to revoke it.

b. If the Personnel Security Branch suspends the clearance, the office provides due process to the employee. This process is explained in paragraph 5 below.

c. After all investigations have been completed; the Personnel Security Branch lifts the suspension or begins additional administrative action. This additional action may include a proposal to revoke the clearance. The Personnel Security Branch includes a written statement describing the action taken and explaining the reasons in the security file.

4. Revoking a security clearance or eligibility. An existing clearance or eligibility is suspended if the Personnel Security Branch proposes to revoke it, and the suspension remains in effect until the Personnel Security Branch makes a final decision on the revocation. The Personnel Security Branch gives notice by letter to the person specifying the reasons for proposing to revoke the clearance, based on the information in the investigation.

a. The letter gives the person 30 calendar days to respond in writing and to request the Personnel Security Branch to review its proposal.

b. The letter informs the person of the right to be represented by counsel or another representative at the individual's own expense. A person may also appear in person before a representative of the Personnel Security Branch to present relevant documents, materials and information. The Personnel Security Branch writes a summary of the appearance and makes it part of the person's security record.

5. Due Process for denying, suspending, or revoking a security clearance or eligibility. The Personnel Security Branch considers all written challenges, replies, or documentation supplied by the person. The Personnel Security Branch compares the responses with the investigation and explains the reasoning for the decision.

a. The Personnel Security Branch arranges for further investigation based on allegations or information in the personnel investigation.

b. Letters of intent to deny, suspend, or revoke a security clearance or eligibility is sent to the person. The letter:

(1) Gives the person 30 calendar days to respond in writing;

(2) Informs the person of the right to be represented by counsel or another representative at the individual's own expense; and

(3) Informs the person that they may appear in person before representatives of the Personnel Security Branch to present relevant documents, materials, and information.

c. The Personnel Security Branch considers all written challenges, replies, or documentation supplied by the person. In making its final decision, the Personnel Security Branch compares the responses with the investigation of allegations, and explains the reasoning for the decision, making this part of the person's security file.

d. The Personnel Security Branch sends a letter to the person with the final decision. In an unfavorable decision, the Personnel Security Branch informs the person of the right to file a written appeal within 30 calendar days.

6. Appeal process. If the person appeals, the OMA Associate Administrator or designee will convene and chair a high-level panel comprised of at least three members, two of whom must be selected from outside the security field.

a. The decision of the appeals panel must be in writing, and will be final, except where the OMA Associate Administrator or designee personally exercises the appeal authority based upon recommendations from the appeals panel.

b. The Personnel Security Branch will then forward the decision to the person's HSSO or RA and attaches a letter to the person for personal delivery by the official's representative. The Personnel Security Branch reinstates the security clearance and files the panel's records in the person's security folder on the shared drive.

c. If the panel upholds the initial decision, the Panel's written decision will be provided to the person's HSSO or RA and the employee will be notified by a letter via personal delivery by the official's representative. If the person is a GSA employee, the memorandum instructs the official to permanently remove the employee from the national security position. The letter explains that the panel's determination is GSA's final decision in the matter. The Personnel Security Branch files the panel's records in the person's security folder on the Personnel Security Branch shared drive.

APPENDIX J. DEFINITIONS

Adjudication: As defined in section 1.3(a) of Executive Order 13467, as amended, adjudication means the evaluation of pertinent data in a background investigation, as well as any other available information that is relevant and reliable, to determine whether a covered individual is:

- Suitable for Government employment;
- Eligible for logical and physical access;
- Eligible for access to classified information;
- Eligible to hold a sensitive position; or
- Fit to perform work for or on behalf of the Government as a Federal employee, contractor, or nonappropriated fund employee.''

Affiliates: Individuals who are not employed (being paid) by GSA, including but not limited to, volunteers, student interns, and summer hires.

Applicant: A person who is being considered, or has been considered, for Federal employment.

Appointee: A person who has entered on duty and is in the first year of employment with the Federal Government.

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

Classified Information: Official information or material that requires protection against unauthorized disclosure in the interest of national security. Information is classified as Confidential, Secret, or Top Secret.

Continuous Evaluation: A vetting process to review the background of an individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. CE leverages a set of automated record checks and business rules to assist in the on-going assessment of an individual's continued eligibility. CE is intended to complement continuous vetting efforts.

Covered Position: As defined in 5 CFR 731.101(b), a covered position means a position in the competitive service, a position in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and a career appointment to a position in the Senior Executive Service.

Critical Sensitive Positions: As defined in 5 CFR 1400.201(a)(2), critical-sensitive positions are, “national security positions which have the potential to cause exceptionally grave damage to the national security.” Also, in accordance with 5 CFR

1400.201(c) a critical-sensitive position automatically carries with it a risk designation under 5 CFR 731.106 at the high level.

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

Deputy Regional Directors (DRD): An employee designated by OMA with the responsibility for administering the security program in their Service or Region.

Electronic Questionnaires for Investigations Processing (e-QIP): A secure web-based system that enables users to create, edit, retrieve, and update personal investigative data as part of the background investigation process.

Fitness: Fitness is the level of character and conduct determined necessary for an individual to perform work for or on behalf of a Federal agency.

National Agency Check (NAC): An investigation consisting of a search of records of the following: OPM Security/Suitability Investigations Index (SII), FBI Name Check and National Criminal History fingerprint check, Department of Defense Clearance and Investigations Index (DCII), and other record searches covering specific areas of an individual's background.

National Security Clearance: A certification issued by personnel security indicating an employee may access classified information on a need-to-know basis.

National Security: As defined in 5 CFR 1400.102(a), national security "refers to those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism."

National Security Information: Information about the U.S. national defense or foreign relations.

National Security Position: As defined in 5 CFR 1400.102(a), a national security position, "includes any position in a department or agency, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security."

Non-critical Sensitive Positions: As defined in 5 CFR 1400.201(a)(1) noncritical-sensitive positions are, "national security positions which have the potential to cause significant or serious damage to the national security." Also, in accordance with 5 CFR 1400.201(d) a noncritical-sensitive position automatically carries with it "a risk designation under 5 CFR 731.106 at the moderate level, unless the agency determines that the position should be designated at the high level. Agencies shall designate the position at the high level where warranted on the basis of criteria set forth in OPM issuances as described in 5 CFR 731.102(c)."

Non-sensitive Position: A position that does not require access to classified information.

Out-of-Scope (overdue): Depending upon the level of access required, individuals holding security clearances are subject to a Periodic Reinvestigation (PR) at a minimum of every five years for Top Secret, 10 years for Secret, and 15 years for Confidential.

Position Designation Automated Tool: An automated tool provided by OPM to assist in determining the level of risk and sensitivity of positions in the competitive service, positions in the excepted service where the incumbent can be noncompetitively converted to competitive service, and initial career appointments in the SES. Position designation determines the type of investigation required for the subject.

Public Trust Position: Positions at the high or 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.

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

Security Clearance: A Top Secret, Secret, or Confidential national security clearance.

Sensitive Position: Any position within or in support of a department or agency, the occupant of which could bring about, by virtue of the nature of the position, a material adverse effect on the national security, regardless of whether the occupant has access to classified information.

Sensitive Compartmented Information (SCI): Classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the DCI.

Sensitivity: A position assessment designation indicating the degree of damage an individual in the position could affect National Security.

Special Sensitive Positions: As defined in 5 CFR 1400.201(a)(3) special-sensitive positions are, "national security positions which have the potential to cause inestimable damage to the national security." Also, in accordance with 5 CFR 1400.201(c) a special-sensitive position automatically carries with it a risk designation under 5 CFR 731.106 at the high level.

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

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

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

Temporary Access/Eligibility: An employee may be granted temporary access to national security information not to exceed 180 calendar days. Temporary eligibility for access is based on minimum investigative standards for a period of 180 calendar days, but continued access will be based on a favorable adjudicated investigation in order to access the level of national security information that is requested.

Waiver: An intentional relinquishment of some right, interest, or the like.

APPENDIX K. REFERENCES

a. Parts 731, 732, and 736 of Title 5, Code of Federal Regulations (CFR). https://www.ecfr.gov/cgi-bin/text-idx?SID=f564b4e3d072d316d15b7b7a35d00fad&mc=true&tpl=/ecfrbrowse/Title05/5cfrv1_02.tpl#0

b. EO 13467, as amended, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified information." June 30, 2008 (Amended by EO 13741, September 29, 2016; EO 13764, January 17, 2017). https://www.gpo.gov/

c. EO 13488, as amended, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust," January 16, 2009(Amended by EO 13764, January 17, 2017). https://www.gpo.gov/

d. EO 13764, "Amending the Civil Service Rules, EO 13488, and EO 13467 to Modernize the Executive Branch-wide Governance Structure and Process for Security Clearance, Suitability and Fitness for Employment, and Credentialing, and Related Matters", January 17, 2017. https://www.gpo.gov/fdsys/pkg/FR-2017-01-23/pdf/2017-01623.pdf

e. EO 12968, as amended, "Access to Classified Information" August 4, 1995(Amended by EO 13467, June 30, 2008). https://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf

f. EO 13526, as amended, "Classified National Security Information," December 29, 2009. https://www.gpo.gov/

g. OPM Memorandum for Heads of Departments and Agencies, Chief Human Capital Officers, and Agency Personnel Security Branch, "Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide," dated January 14, 2008. https://www.opm.gov/suitability/suitability-executive-agent/policy/decision-making-guide.pdf

h. OPM Memorandum for Heads of Departments and Agencies, Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12," dated July 31, 2008.

https://www.opm.gov/suitability/suitability-executive-agent/policy/final-credentialing-standards.pdf

i. 32 CFR Part 147, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information. http://www.gpo.gov/fdsys/pkg/CFR-2011-title32-vol1/pdf/CFR-2011-title32-vol1-part147.pdf

j. OPM Position Designation System and Automated Tool. https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/

k. Homeland Security Presidential Directive-12 (HSPD-12) - Policy for a Common Identification Standard for Federal Employees and Contractors, as it applies to GSA. August 27, 2004. https://www.dhs.gov/homeland-security-presidential-directive-12

l. Security Executive Agent Directive (SEAD) 3. Reporting Requirements for Personnel with Access to Classified Information or Who Hold A Sensitive Position. June 12, 2017. https://www.dm.usda.gov/ohsec/docs/SEAD%203%20Reporting%20(U).pdf

m. Security Executive Agent Directive (SEAD) 4. National Security Adjudicative Guidelines. June 8, 2017. http://ogc.osd.mil/doha/SEAD4_20170608.pdf

n. Security Executive Agent Directive (SEAD) 6. Continuous Evaluation Program. January 12, 2018. https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-6-continuous%20evaluation-U.pdf

o. SEAD 7. Reciprocity of Background Investigations and National Security Adjudications. November 9, 2018. https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf

p. CPO 9751.1 (Revalidated) Maintaining Discipline, May 20, 2003; Revalidated August 22, 2013. https://www.gsa.gov/cdnstatic/Directives/OAS_57401_CHGE_1_Government_Travel_Charge_Card_Program_%28Posted_Version_-_12-1-2017%29_RV_%23CC037614.pdf

q. 5 CFR Part 1400 – Designation of National Security Positions. https://www.gpo.gov/fdsys/granule/CFR-2016-title5-vol3/CFR-2016-title5-vol3-part1400

APPENDIX L. ACRONYMS

Acronym	Meaning
CFR	Code of Federal Regulations
CPX	Executive Resources Division
e-OPF	Electronic Official Personnel Folder
e-QIP	Electronic Questionnaires for Investigations Processing
EO	Executive Order
EOD	Entrance on Duty
FBI	Federal Bureau of Investigation
HSPD-12	Homeland Security Presidential Directive-12
INV 79A	Report of Agency Adjudicative Action
ODNI	Office of the Director of National Intelligence
OHRM	Office of Human Resource Management
OPM	Office of Personnel Management
PAL	Proposed Action Letter
PD	Position Description
PII	Personally Identifiable Information
PIPS	Personnel Investigations Processing System
ROI	Report of Investigation
SAC	Special Agreement Checks
SAP	Special Access Programs
SCI	Sensitive Compartmented Information
SES	Senior Executive Service
SHRO	Servicing Human Resources Offices
USC	United States Code