



| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

NASA Procedural Requirements

NPR 1600.3A

Effective Date: August 03, 2020

Expiration Date: August 03,
2025

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Personnel Security

Responsible Office: Office of Protective Services

Table of Contents

Preface

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents and Forms
- P.5 Measurement/Verification
- P.6 Cancellation

Chapter 1. Introduction

- 1.1 Overview
- 1.2 Scope
- 1.3 Roles and Responsibilities
- 1.4 Violations of Security Requirements

Chapter 2. Personnel Security Investigations and Adjudications

- 2.1 General
- 2.2 Risk and Sensitivity Levels
- 2.3 Designation of Risk and Sensitivity Levels
- 2.4 Non-U.S. Citizens
- 2.5 Childcare Providers
- 2.6 Investigation Process Requirements
- 2.7 Reinvestigation
- 2.8 Reciprocity of Investigations and Adjudications
- 2.9 Adjudications

2.10 Personnel Security File Storage and Access

Chapter 3. Personnel Security for National Security Positions

3.1 General

3.2 Reciprocity of National Security Investigations and Adjudications

3.3 Adjudication

3.4 Suspension

3.5 Denial or Revocation

3.6 Continuous Evaluation

3.7 Sensitive Compartmented Information (SCI)

3.8 One-Time Access to CNSI

3.9 Temporary/Interim Access to CNSI

3.10 Limited Access to CNSI by Non-U.S. Citizens

3.11 Access to Restricted Data (RD) or Formerly Restricted Data (FRD)

Appendix A. Definitions

Appendix B. Acronyms

Appendix C. References

Preface

P.1 Purpose

- a. This directive describes the Agency-wide personnel security program implementation requirements set forth in NASA Policy Directive (NPD) 1600.2, NASA Security Policy, as amended.
- b. This directive prescribes personnel security program responsibilities and procedural requirements for personnel security investigations, determinations of eligibility for access to Classified National Security Information (CNSI) and to hold a sensitive position, continuous evaluation, contractor fitness, adjudication, and appeals of NASA Federal and contractor employees.

P.2 Applicability

- a. This directive is applicable to NASA Headquarters and all NASA Centers, including Component Facilities and Technical and Service Support Centers. This directive applies to the Jet Propulsion Laboratory (JPL) (a Federally Funded Research and Development Center (FFRDC)), other contractors, recipients of grants, cooperative agreements, or other agreements only to the extent specified or referenced in the applicable contracts, grants, or agreements.
- b. This directive is applicable to all NASA civil service employees, NASA contractor employees, personnel completing work through Space Act Agreements, those assigned or detailed under the Intergovernmental Personnel Act, partners, recipients of grants and cooperative agreements or other agreements, and visitors.
- c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term “shall.” The terms: “may” or “can” denote discretionary privilege or permission, “should” denotes a good practice and is recommended, but not required, “will” denotes expected outcome, and “are/is” denotes descriptive materials.
- d. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

P.3 Authority

Security Requirements, 51 United States Code (U.S.C.) § 20132.

P.4 Applicable Documents and Forms

- a. Freedom of Information Act, 5 U.S.C. § 552.
- b. Privacy Act of 1974, 5 U.S.C. § 552a.
- c. Violation of Regulations of National Aeronautics and Space Administration, 18 U.S.C. § 799.
- d. Equal Employment Opportunity, E.O. 11246, 3 CFR 1964-1965 (1965).

- e. National Industrial Security Program, E.O. 12829, 3 CFR 1993 Comp. (1993).
- f. Access to Classified Information, E.O. 12968, 3 CFR 1995 Comp. (1995).
- g. Suitability, 5 CFR pt. 731.
- h. NPD 1600.2, NASA Security Policy.
- i. NPR 1441.1, NASA Records Management Program Requirements.
- j. NPR 1600.2, NASA Classified National Security Information (CNSI).
- k. NPR 1600.4, Identity and Credential Management.
- l. NPR 3730.1, NASA Suitability Program.
- m. Department of Defense (DOD) Manual 5220.22, Volume (Vol.) 2, National Industrial Security Program: Industrial Security Procedures for Government Activities (August 1, 2018).
- n. Presidential Policy Directive (PPD) 19, Protecting Whistleblowers with Access to Classified Information (October 10, 2012).
- o. Security Executive Agent Directive (SEAD) 4, National Adjudicative Guidelines (June 8, 2017).

P.5 Measurement/Verification

- a. Compliance with this NPR will be accomplished by Agency-wide application of uniform suitability, eligibility, contractor fitness, and adjudication procedures that foster reciprocity, reduce duplication efforts, and ensure consistent quality standards for adjudication procedures. Measurement of compliance will rely upon objective and modern analytic methods rather than practices that avoid risk.
- b. Reviews of personnel security program policies and procedures will be conducted in accordance with NPR 1600.1 for Functional Review of Centers.
- c. The Office of Protective Services (OPS) audits, conducts Functional Reviews of the Centers, and conducts spot-checks and inspections to review Center compliance and implementation of this NPR. OPS audits/reviews are conducted at least every three years or sooner, as required, to determine compliance with this NPR. The findings of the audits/reviews are provided to the applicable Center Director for resolution no later than 30 days from the completion of the reviews/audits.

P.6 Cancellation

NPR 1600.3, Personnel Security, dated April 29, 2013.

Chapter 1. Introduction

1.1 Overview

1.1.1 This NASA directive establishes the policies and high-level procedures used throughout NASA to achieve consistency in personnel security. Strong, personnel security processes and practices, adhering to Federal requirements and guidance, support a secure environment where trusted individuals are granted appropriate access to approved assets in order to conduct business.

1.1.2 Personnel security processes and practices include all the activities necessary to investigate and adjudicate personnel security investigations, including position designations, reinvestigation, and continuous evaluation.

1.1.3 Personnel security investigations (PSI), also referred to as investigations, are used to evaluate the character and conduct of all NASA workers to determine suitability for Government employment, fitness for contractor employees, and eligibility for access to Federal facilities, federally controlled information systems, and classified national security information (CNSI), and eligibility to hold a sensitive position.

1.2 Scope

1.2.1 The policies and procedures identified within this document define the approved processes for NASA to manage a personnel security program. The personnel security program includes all investigations and adjudications for determining eligibility for access to non-sensitive and sensitive assets.

1.2.2 NASA requirements for suitability are covered by NPR 3730.1, NASA Suitability Program.

1.3 Roles and Responsibilities

1.3.1 The NASA Administrator shall implement a comprehensive and effective personnel security program for the Agency.

1.3.2 The Assistant Administrator, Office of Protective Services (AA, OPS) shall:

- a. Establish and maintain an efficient, comprehensive, and effective personnel security program and associated personnel security policy, in accordance with Federal standards consistent with current personnel security/fitness policies, procedural requirements, and guidelines as established by the Office of the Director of National Intelligence (ODNI), and the Office of Personnel Management (OPM).
- b. Serve as the Agency Advocate for the investigative and adjudicative systems of record.
- c. Approve pre-appointment waivers for persons to occupy sensitive positions pending final investigation and adjudication.

1.3.3 The Director, OPS Security Management Division (OPS/SMD) shall:

- a. Serve as the Agency administrator and primary point of contact to OPM and ODNI.
- b. Execute the personnel security program established by the AA, OPS.
- c. Oversee the suitability determinations for first-time NASA civil service employees occupying a sensitive position.
- d. Oversee the fitness determinations of all NASA contractors.
- e. Oversee the physical and logical access determinations of all NASA workers.
- f. Manage and oversee the Agency capability for determining eligibility for access to CNSI and/or to occupy a sensitive position.
- g. Review and assess Center compliance with personnel security requirements established in this policy through functional reviews and/or audits of Center personnel security programs.

1.3.4 The Office of the Chief Human Capital Officer (OCHCO) shall:

- a. Establish policies and oversee activities related to determining risk and sensitivity for all NASA civil service employees.
- b. Establish policies and oversee activities related to determining suitability for NASA civil service employees occupying low-risk and public trust positions.
- c. Cooperate with security officials during security inquiries and investigations pertaining to the requirements of this policy.

1.3.5 The NASA Management Office (NMO) Director shall perform the role of Center Director at JPL for the purposes of this NPR.

1.3.6 Center Directors shall ensure full Center compliance with the provisions set forth in this NPR.

1.3.7 The Center Chief of Security (CCS)/Center Chief of Protective Services (CCPS) shall:

- a. Oversee the personnel security program at their Center.
- b. Designate a Federal civil service employee with a favorably adjudicated PSI to serve in the role of Program Manager for the investigative and adjudicative systems of record.
- c. Ensure adjudications for credentialing is performed by senior personnel security specialists who have been trained and certified in accordance with Federal training standards.

1.3.8 Personnel Security Specialists shall:

- a. Process and submit all PSI requests electronically using the investigative questionnaire system of record.
- b. Ensure that a check of investigative and adjudicative systems of record are performed to validate any prior investigation or adjudication that will meet reciprocity standards before initiating a PSI.
- c. Maintain close coordination with the investigative service provider (ISP) and process requests for PSIs.
- d. Perform adjudications for credentialing, suitability, fitness, and access to CNSI.

- e. Initiate requests for access to CNSI and/or to occupy a sensitive position for NASA workers under their jurisdiction.
- f. Notify the Director, OPS/SMD, or designee, of any adverse information regarding any NASA workers at the Center that have access to CNSI or occupy a sensitive position.
- g. Recommend suspension of a NASA worker's eligibility for access to CNSI and/or to hold a sensitive position based on developed disqualifying adverse information, as detailed in this NPR.
- h. Perform an annual review of NASA workers with access to CNSI and access requirements to ensure Center personnel security access needs are properly managed. The CCS/CCPS will develop and implement local procedures necessary to ensure the review is conducted.
- i. In cooperation with OCHCO Resource Specialists, determine the risk and sensitivity of all positions requiring eligibility for access to CNSI.
- j. Refer all developed adverse information for NASA civil service employees to OCHCO personnel for review.
- k. Conduct National Criminal History Checks (NCHC) and other local records checks or automated record checks.
- l. In cooperation with OCHCO, conduct local records checks or automated record checks to clarify, expand, or mitigate information that has been provided by the investigation provider or a Department of Justice, National Crime Information Center (NCIC) query, when requested.
- m. Maintain, in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a and existing NASA system of records, personnel security files on all investigated personnel.
- n. Review reports with officials in the review process who make the determination relative to continued access or revocation of access privileges.
- o. Inform all investigated personnel of their rights to request, in compliance with the Freedom of Information Act, 5 U.S.C. § 552 any documents, records, and reports upon which an investigation was conducted.

1.3.9 National Security Adjudicators shall:

- a. Ensure that a check of investigative and adjudicative systems of record are performed to validate any prior investigation or adjudication that will meet reciprocity standards before initiating a PSI.
- b. Maintain close coordination with the ISP and process requests for PSIs.
- c. Process requests for access to CNSI for all NASA workers.
- d. Determine suitability for NASA civil service employees occupying sensitive positions.
- e. Perform adjudications to determine eligibility for access to CNSI and/or to occupy a sensitive position.
- f. Suspend, revoke, or deny a NASA worker's eligibility for access to CNSI and/or to occupy a sensitive position.
- g. Maintain, in accordance with the Pub. L. 93-579 and existing NASA system of records, personnel security files on all personnel with access to CNSI and/or who occupy a sensitive position.

h. Coordinate and communicate with Center personnel security specialists regarding civil servant eligibility for access to CNSI.

1.3.10 Managers and supervisors shall ensure full compliance with the requirements established in this policy and OCHCO policy for suitability.

1.3.11 The NASA General Counsel or the Chief Counsel of each Center shall provide legal counsel as required within this policy.

1.3.12 Contract Management Officials (Contractor Management, Contracting Officer (CO), Contracting Officer's Representative (COR), and Project Managers) shall:

a. Ensure full compliance with the requirements established in this policy.

b. Coordinate with the CCS/CCPS for the designation of risk and sensitivity, and the onboarding of contractor employees.

1.4 Violations of Security Requirements

1.4.1 Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving the NASA personnel security program is subject to disciplinary action up to and including termination of employment and/or prosecution under the Violation of Regulations of National Aeronautics and Space Administration, 18 U.S.C. § 799, and provides fines or imprisonment for not more than one year, or both.

Chapter 2. Personnel Security Investigations and Adjudications

2.1 General

2.1.1 Individuals who perform work for or on behalf of the Agency shall be assigned to a position that has been designated in accordance with OPM position designation requirements.

2.1.2 Individuals who perform work for or on behalf of the Agency are subject to a PSI, in accordance with their assigned position, to determine whether they are:

- a. Suitable for Government employment.
- b. Eligible for logical and physical access.
- c. Eligible for access to CNSI.
- d. Eligible to hold a sensitive position.
- e. Fit to perform work for or on behalf of the Government as a contractor employee.

2.1.3 A determination of suitability for Government employment for all NASA civil service employees, fitness for all NASA contractor employees, and eligibility for logical and physical access will apply to all NASA workers in accordance with NPR 3730.1 and NPR 1600.4, Identity and Credential Management. A determination of eligibility for access to CNSI and/or to hold a sensitive position may apply to NASA workers, in accordance with this policy and NPR 3730.1.

2.1.4 All information obtained regarding personnel security reports and/or records will be handled in accordance with the Privacy Act of 1974.

2.1.5 Intergovernmental Personnel Act (IPA) personnel shall be adjudicated for access based on their position designation.

2.1.6 Prior favorable suitability, fitness, and national security determinations will be reciprocated for that investigation tier and lower investigation tiers in compliance with the requirements for reciprocity found in this policy and NPR 3730.1.

2.1.7 A NASA worker who requires a higher tier of investigation will be subject to a new investigation commensurate with the requirements of the higher tier investigation.

2.1.8 All persons with a PSI will be continuously evaluated to ensure continued suitability/fitness and/or eligibility.

2.1.9 All investigations will be processed using approved Federal Government systems, in compliance with policies for the use of these systems.

2.1.10 The Identity Management and Account Exchange (IdMAX) system will be the authoritative system for tracking, initiation, and adjudication of investigations.

2.1.11 IdMAX will be the authoritative system for position designations of contractors. Position

designations for NASA is maintained by OCHCO.

2.2 Risk and Sensitivity Levels

2.2.1 Position risk will be designated as Low-Risk, Moderate-Risk, or High-Risk.

2.2.1.1 Positions designated as Moderate-Risk or High-Risk will be referred to as Public Trust positions.

2.2.1.2 High-Risk positions will be a minimum Tier 4 investigation.

2.2.1.3 Moderate-Risk positions will be a minimum Tier 2 investigation.

2.2.1.4 Low-Risk positions will be a Tier 1 investigation, except when elevated by the position sensitivity.

2.2.2 Position sensitivity levels will be designated as Non-Sensitive, Non-Critical Sensitive, Critical-Sensitive, or Special-Sensitive.

2.2.2.1 Critical-Sensitive and Special-Sensitive positions will be a Tier 5 investigation.

2.2.2.2 Non-Critical Sensitive positions will be a minimum Tier 3 investigation.

2.2.2.3 Non-Sensitive positions will be a Tier 1 investigation, except when elevated by the position risk.

2.3 Designation of Risk and Sensitivity Levels

2.3.1 All position designations will be made using the approved Federal Government position designation tool.

2.3.2 Position designations for civil service employees will be made by OCHCO in coordination with the supervisor and OPS.

2.3.3 Position designations for contracts, grants, cooperative agreements, and Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) will be made by the responsible NASA Center program office representative; typically, by the designated civil service project manager (sponsor/requester), COR, in coordination with OPS, and Information Technology Security Manager(s) and in compliance with position designation standards.

2.3.4 Position designations for national security contracts will be made in accordance with NPR 1600.2, NASA Procedural Requirements.

2.3.5 The risk and sensitivity level for contractor positions will be identified and designated in the statement of work of the contract.

2.3.6 If the duties of a position require overlap into a higher or lower risk level, the position risk will be set at the highest risk level anticipated.

2.3.6.1 The COR, in consultation with the CO, will identify contract employees to be processed at each risk level designation and will specify the duties of the contractors. In instances where there is a wide variance in the security risk level of the work to be performed, individual contractor employees

will be processed at the risk designation commensurate with the highest risk level of their duties.

2.3.6.2 An entire contract, grant, MOA, or MOU may be designated high or moderate risk, but those NASA contractor employees whose work would be moderate or low risk will be investigated according to the highest risk level of their duties. In meeting this contingency, the contract, grant, MOA, or MOU will specifically apply controls to ensure that work of the lower-risk positions does not overlap with that for the higher-risk positions.

2.4 Non-U.S. Citizens

2.4.1 Non-United States (U.S.) citizens, including Lawful Permanent Residents (LPR), are eligible for placement in low-risk and moderate-risk positions, but are not normally eligible for employment in positions designated as high-risk. Appointments to these positions will follow the requirements of NPR 3300.1.

2.4.2 Non-U.S. citizens residing in the U.S. for less than three years are ineligible for a background investigation and appointment to any low-risk, moderate-risk, or high-risk position.

2.5 Childcare Providers

2.5.1 A Tier 1 investigation, or higher, will be completed on all childcare providers. The appropriate extra coverage code will be requested during the initiation of the investigation for childcare providers.

2.5.2 NASA childcare facilities will coordinate all personnel hiring actions with OPS prior to the start of employment.

2.6 Investigation Process Requirements

2.6.1 An investigation is initiated for all NASA workers, commensurate with the position risk and sensitivity.

2.6.2 The applicant shall submit fingerprints through the IdMAX system.

2.6.3 The applicant shall submit all necessary information and forms that may be required, based on the type of investigation, and then sign the appropriate release pages.

2.6.4 Investigation forms will be certified and submitted to the ISP within 14 days of signature by the applicant.

2.6.5 If the required investigation is determined to have not been accomplished at any time, the required investigation will be conducted.

2.6.6 At the discretion of OPS, an individual without a completed investigation and final access determination may be allowed to begin work based on the specifics of the situation and a preliminary review of the submitted forms and the results of the fingerprint check.

2.6.7 Changes in Position, Risk, or Sensitivity Level.

2.6.7.1 When a NASA worker experiences a change in work duties and the risk or sensitivity level is

higher, a new investigation commensurate to the risk or sensitivity will be transmitted to the ISP.

2.6.7.2 When a NASA worker experiences a change in work duties and the risk or sensitivity level is lower, the existing investigation will be accepted with no additional action.

2.7 Reinvestigation

2.7.1 Tier 1 investigations are not subject to periodic reinvestigation.

2.7.2 Tier 2, 3, 4, and 5 investigations will be reinvestigated and/or evaluated in accordance with Federal policies.

2.7.3 Reinvestigations, including expanded or further investigations because of continuous evaluation, will be conducted when required, consistent with the Federal Investigation Standards.

2.8 Reciprocity of Investigations and Adjudications

2.8.1 The investigative and adjudicative systems of record are checked by a NASA personnel security specialist who has undergone a favorably adjudicated PSI to determine if a prior investigation or adjudication will serve reciprocally for a NASA determination of suitability, fitness, or access to physical and logical resources. If there is no favorably adjudicated PSI identified in an adjudicative system of record, or any other trusted Government agency that will serve reciprocally, a PSI will be initiated in the investigative questionnaire system of record commensurate to the position risk and sensitivity.

2.8.2 Reciprocal recognition will be granted for a prior favorable suitability, fitness, or access determination when:

- a. Equivalent adjudicative criteria was used in accordance with Suitability, 5 CFR pt. 731; and
- b. The individual has had no break in employment since the favorable determination was made.
- c. The new position requires the same or a lower level of investigation than previously conducted for that individual; or
- d. No developed adverse information has been obtained on the individual; or
- e. The individual's investigative record does not reflect conduct that is incompatible with the core duties of the new position; or
- f. The investigation is within the same scope.

2.9 Adjudications

2.9.1 Adjudications will be performed in accordance with Federal guidelines for credentialing, suitability, and eligibility for access to CNSI and/or to hold a sensitive position.

2.9.2 Adjudications are made by certified credentialing adjudicators in accordance with suitability/fitness adjudication standards.

2.9.3 Adjudicative decisions will be made on individuals whom an appropriate investigation has

been completed.

2.9.4 Adjudicative decisions are made in accordance with Federal adjudicative standards.

2.9.5 Adjudications are performed within the established timelines identified in Federal guidelines and recorded in IdMAX.

2.9.6 Adverse Information

2.9.6.1 When adverse information is developed or received in the course of any personnel security investigation, subsequent to such investigation and initial favorable determination, or through continuous evaluation, the scope of inquiry will be expanded to the extent necessary to obtain sufficient information to make a reasonable and sound determination to obtain or maintain suitability, fitness, or eligibility for access.

2.9.6.2 A personal interview or expanded inquiry is held with a NASA worker on whom significant unfavorable or derogatory information has been developed or received during the screening process. The NASA worker will be offered an opportunity to refute, explain, clarify, or mitigate the information in question. As appropriate, other offices will be consulted (e.g., OIG, OGC, OCHCO, etc.) during this process.

2.9.6.3 Expanded inquiries or personal interviews will be conducted by a NASA official with sufficient investigative experience, NASA-contracted investigators, another investigating agency, or another agency of the Federal Government at NASA's request.

2.9.6.3.1 Signed releases from the NASA worker are obtained when required to pursue additional leads, such as medical records, credit checks, etc.

2.9.6.4 Counterintelligence-related adverse information is relayed immediately, but no later than the next business day after the information has been obtained, to OPS Counterintelligence and Counterterrorism.

2.9.6.5 An adjudicator shall conduct a new determination at any time adverse information is obtained that calls into question an individual's fitness, suitability, or eligibility for access based on character or conduct. This may include a new PSI or database query and adjudication. Adverse information involving civil service employees will be referred to OCHCO for action.

2.9.6.6 The adjudicator shall provide the individual a notice stating the specific reasons for the determination and that the individual has the right to answer the notice in writing. The notice will inform the individual of the time limits, as well as the address to which the response should be made.

2.9.6.7 The individual may respond to the determination in writing and furnish documentation that addresses the specific reasons for the determination in support of the response. If no response is received, the determination will be upheld and there will be no further appeal process.

2.9.6.8 After consideration of any documentation submitted by the individual for reconsideration of the initial determination, OPS shall issue a written decision, which informs the individual of the reasons for the final decision. If the letter details an unfavorable decision, the individual may request an appeal within the defined time limit.

2.9.6.9 The Center Director, or designee, shall appoint a Credentialing/Fitness Adjudication Review Panel (CARP) to review the information surrounding the denial decision. The panel will be

composed of three NASA civil servants who have demonstrated reliability and objectivity in their official duties. One, and only one, of the panel members must be a security professional. If use of a NASA security professional is not appropriate, a security expert from outside the Agency may be used on the panel. The individual may submit a written appeal to the CARP or they may request to appeal in person to the CARP. Any approved appearance before the CARP will be documented by means of a written summary or recording which will be made a part of the individual's security record.

2.9.6.10 Prior to finalizing the CARP determination, a CARP panel member or OPS may refer the CARP proposed decision to the Center Director for an additional level of review. If no referral is made to the Center Director, the CARP decision is final. If there is a referral to the Center Director, the Center Director's decision is final.

2.9.6.11 Upon determination that a denial has been upheld, there is no further appeal process.

2.9.6.12 Based on the reasons for the denial, the individual may be barred from access to NASA. IdMAX will be updated to reflect any barring of access.

2.9.6.13 If at any point during review and/or adjudication of adverse information the individual's affiliation with NASA ends, no further action is required and the review process should be concluded.

2.10 Personnel Security File Storage and Access

2.10.1 Records and information related to this policy will be managed in accordance with NPR 1441.1. Personnel security files are temporary records and are to be destroyed in accordance with the disposition instructions in NPR 1441.1.

2.10.2 Information from personnel security files may be disclosed to a Federal agency in response to requests to the extent that the information is appropriate for release to the requesting official, relevant, and necessary to the requesting agency's decision on the matter.

2.10.3 Subjects of personnel security investigations and screenings may request copies of excerpts, summaries, or any analytical extract of information from the NASA case file or the investigation in accordance with the Freedom of Information Act and the Privacy Act of 1974. The subject may be directed to make such requests directly to the ISP.

2.10.4 The results of PSIs will be used by NASA for the limited purpose of making suitability, fitness, and/or eligibility determinations.

2.10.5 Adjudicative determinations are reported using the officially designated system.

2.10.6 NASA Personnel Security Specialists shall only access PSI and adjudicative records relevant to the specific individual for whom a hiring, credentialing, or eligibility determination is required. PSI and adjudicative records may be accessed at the direction of the Director, OPS/SMD or designee. PSI and adjudicative records will only be accessed through officially designated systems.

2.10.7 All records related to PSIs, database checks, screening records, adjudicative decisions, or similar personnel security files are maintained securely.

Chapter 3. Personnel Security for Sensitive Positions

3.1 General

3.1.1 The personnel security program will ensure that only loyal, trustworthy, and reliable people are granted access to CNSI or assigned to sensitive positions.

3.1.2 All NASA civil service employees occupying a sensitive position are investigated and adjudicated for eligibility to hold a sensitive position, consistent with Federal requirements.

3.1.3 All NASA employees requiring initial or continuing access to CNSI are investigated and adjudicated for eligibility to access CNSI, consistent with Federal requirements.

3.1.4 NASA contractors requiring access to CNSI will be processed in accordance with NPR 1600.2 and the requirements of E.O. 12829, the National Industrial Security Program Operating Manual (NISPOM) and NISPOM Supplement.

3.1.5 Foreign nationals requiring access to CNSI will be processed in accordance with NPR 1600.2 and the requirements of DOD Manual 5220.22, Vol. 2.

3.1.6 All NASA workers requiring access to Sensitive Compartmented Information (SCI) will be processed in accordance with this policy and NPR 1600.2.

3.1.7 OPS shall implement an annual revalidation of access to CNSI whereby personnel who have not had the need to access CNSI during the previous year will be given serious consideration for administrative withdrawal of their eligibility for access to CNSI as determined by supervisors during the revalidation process.

3.1.8 No individual will be given access to CNSI or assigned to a sensitive position unless a favorable eligibility determination has been made.

3.1.9 The NASA Central Adjudication Facility (CAF), in coordination with security office personnel and supervisors and OCHCO, shall make employment suitability determinations for individuals entering the Federal workforce and holding a sensitive position.

3.1.10 Subjects of adjudications are notified when an interim or final eligibility decision has been made, or reciprocity of an existing adjudication has been accepted.

3.1.11 Subjects of adjudications, including denial and revocation, may refute any information developed during the investigation process that may result in an ineligibility for access to CNSI.

3.1.12 Requests for access to CNSI will result in an adjudicative determination unless, unrelated to any potential adjudication factor, the need for access no longer exists (e.g., change of position, termination of employment, etc.).

3.1.13 The policies and procedures for suspension, denial, and revocation are not to be confused with the procedures for the removal of a NASA worker on national security grounds as set forth in 5 U.S.C. § 7532, Suspension and Removal. OPS will coordinate with OCHCO to pursue the removal

of a NASA worker on national security grounds regardless of the NASA worker's position sensitivity or access to CNSI.

3.2 Reciprocity of National Security Investigations and Adjudications

3.2.1 Reciprocity will follow the requirements established in section 2.8, Reciprocity of Investigations and Adjudications.

3.2.2 Reciprocity will be granted in accordance with SEAD-7.

3.3 Adjudication

3.3.1 Adjudications follow all relevant Federal policies and regulations, including but not limited to the Security Executive Agent Directive (SEAD) 4.

3.3.2 Adjudications are fully documented and recorded in the subject's security file and entered into the adjudicative system of record.

3.3.3 All reasonable efforts will be pursued to develop potential issue information, as well as potentially favorable or mitigating information.

3.3.4 Adjudications will be made by certified national security adjudicators in accordance with National Security Adjudication Standards.

3.3.5 Adjudications for first-time access are performed on closed investigations commensurate with the required access.

3.3.6 Adjudications will be evaluated continuously against all new information obtained subsequent to the initial national security adjudication and in compliance with Federal standards.

3.4 Suspension

3.4.1 The AA, OPS, or designee, shall make all suspension determinations.

3.4.2 The CCS/CCPS shall propose suspensions of security clearances to the NASA CAF for cause based on developed adverse information.

3.4.3 The AA, OPS, or designee, shall make a final determination after consultation with the NASA CAF and the Office of the General Counsel (OGC).

3.4.4 The AA, OPS, or designee, shall suspend an individual's security clearance when information is developed that suggests the individual's continued access to CNSI is not in the interest of national security.

3.4.5 The subject of a suspension does not need to be provided with a reason or reasons for the suspension and will be notified.

3.4.6 Suspensions should not be open-ended. Every effort should be expended to complete subsequent investigations and adjudications as soon as practical. All suspension actions should be

resolved as soon as practical from the date of the suspension.

3.4.7 Suspension of an individual's access to CNSI allows the Agency sufficient time to investigate and adjudicate information that may affect the individual's eligibility for access to CNSI.

3.4.8 The subject of a suspension will not be entitled to review procedures.

3.4.9 The NASA CAF shall determine whether to reinstate or revoke the clearance upon receipt of information containing documented facts relating to the suspension. Revocations will follow the requirements in section 3.5, Denial or Revocation.

3.5 Denial or Revocation

3.5.1 In the event of a denial or revocation, the subject is entitled to obtain a review of the decision.

3.5.2 Only the AA, OPS, or designee, shall make a denial or revocation determination.

3.5.3 In the event of an unfavorable adjudication action, the NASA CAF shall propose documented reasons in a Letter of Intent (LOI) to deny or revoke eligibility for access to CNSI and/or to hold a sensitive position.

3.5.4 The Director, Security Management Division (DSMD), shall review the proposed unfavorable adjudicative action by CAF personnel and:

a. Remand the case for further work; or

b. Uphold the proposed adjudication of the information, and in consultation with the Office of the Inspector General (OIG), provide written notice to the subject of the denial or revocation through an OPS designee.

3.5.5 The employee shall acknowledge receipt of the LOI and respond within the time specified in the LOI or request an extension, if warranted. If the subject provides new information for consideration, the NASA CAF will review the new information provided. The NASA CAF will make a recommendation to the DSMD whether access to CNSI should be reinstated, revoked, or denied. If inadequate or no information is provided or no response is provided within the specified time allowed, the NASA CAF will continue with the denial or revocation process. Upon completion of the process, the subject will be notified by the DSMD of a final decision in a Letter of Notification (LON). The letter is served through the OPS designee.

3.5.6 The employee may request an appeal of the initial determination by the DSMD within the timeframe specified in the LON. The employee may submit an appeal in writing or request an in person or virtual hearing by the AA, OPS. The subject may seek private legal representation. The AA, OPS shall review the initial determination (LON or Revocation) and any information submitted by the subject on appeal. The AA, OPS shall ensure that the rights of the subject are protected and due process is accorded. The AA, OPS will document the process by means of a written summary, recording, or similar record, which will be made a part of the subject's security record.

3.5.7 If the AA, OPS provides a notice of denial or revocation and the subject subsequently requests an appeal by a Security Adjudication Review Panel (SARP), the NASA Administrator, or designee, will appoint that body. The panel will be composed of three NASA civil service employees who have demonstrated reliability and objectivity in their official duties. Panel members will have a favorable Tier 5, and only one of the panel members may be a security professional. If use of a

NASA security professional is not appropriate, a security expert from outside the Agency may be used on the panel. The subject may submit a written appeal to the SARP or they may choose to appeal in-person or virtually to the SARP. Any personal appearance before the SARP will be documented by means of a written summary or recording which will be made a part of the subject's security record.

3.5.8 Prior to finalizing the SARP determination, a SARP panel member or the AA, OPS may refer the SARP proposed decision to the Administrator, or designee, for an additional level of review. If no referral is made to the Administrator, the SARP decision is final. If there is a referral to the Administrator, the Administrator's decision is the final Agency decision.

3.5.8.1 Protecting Whistleblowers with Access to Classified Information.

3.5.8.1.1 Any allegations made by an employee in accordance with PPD-19 shall be forwarded to the OIG for review, under procedures as the OIG may separately prescribe. The employee may request an external review by a three-member Inspector General panel, which may be granted per PPD-19, section C in the sole discretion of the Inspector General of the Intelligence Community. The NASA Administrator, or designee, shall carefully consider the findings of and actions recommended by any external review panel.

3.5.8.1.2 In his sole discretion, the AA, OPS may await the review of the employee's case prior to making a determination or may suspend or revoke the employee's eligibility for access to CNSI and/or to hold a sensitive position pending a report by the NASA OIG or the external review panel. Any report provided will be considered by the AA, OPS, including consideration of reinstating a revoked or suspended eligibility for access to CNSI and/or to hold a sensitive position.

3.5.9 Upon determination that a revocation or denial has been upheld, the case will be referred to OCHCO for NASA civil servants.

3.6 Continuous Evaluation

3.6.1 All cleared individuals are subject to a continuous evaluation of their qualifications to meet the high standards of conduct expected of persons in sensitive positions.

3.6.2 Persons subject to a prior favorable personnel security determination who demonstrate behavior that places doubt on their loyalty, reliability, or trustworthiness or otherwise disqualifies that individual for continued access and/or eligibility will be subject to further scrutiny and possible suspension of access to CNSI.

3.6.3 OPS shall conduct fact finding of any reports of disqualifying conduct. Depending on the adverse impact to national security, an individual's eligibility for access to CNSI and/or to occupy a sensitive position may be suspended for cause. A periodic assessment or other PSI to support the assessment of the NASA worker's continued eligibility for access to CNSI and/or to occupy a sensitive position may be requested. The NASA CAF will determine if the individual continues to be eligible for access to CNSI and/or to occupy a sensitive position.

3.6.4 Foreign travel and contacts, both official and unofficial, are reported and tracked in accordance with NPR 1600.2.

3.6.5 Foreign travel and contacts, both official and unofficial, will be reviewed by the NASA CAF as part of the continuous evaluation program.

3.6.6 Information developed during the continuous evaluation process may not be shared with the Center OCHCO or management while the evaluation is pending. The AA, OPS, or designee, may override this principle, if, in their judgment, the information suggests that the subject poses an immediate and serious threat to the health or safety of other individuals, is a threat to a critical mission, or shall otherwise be ineligible for or lose continuation of Federal employment.

3.7 Sensitive Compartmented Information (SCI)

3.7.1 Candidates for access to SCI will occupy a position designated as special-sensitive.

3.7.2 Candidates for access to SCI will have a favorably adjudicated Top Secret (TS) investigation.

3.7.3 The NASA CAF shall manage and submit to the cognizant security authority all information required to make a determination of eligibility for access to SCI.

3.8 One-Time Access to CNSI

3.8.1 One-time access determinations will only be granted by the NASA CAF in accordance with Federal guidelines.

3.8.2 One-time access determinations will only be granted to individuals whose expertise offers specialized and important benefit and value to NASA.

3.8.3 One-time access determinations may be issued for up to one year.

3.8.4 Extensions will not be granted for one-time access determinations.

3.8.5 One-time access determinations will only be granted to U.S. citizens.

3.8.6 The NASA CAF shall maintain all records related to one-time access determinations.

3.9 Temporary/Interim Access to CNSI

3.9.1 Temporary access (also referred to as interim access) to CNSI will only be granted by the AA, OPS, or designee, in accordance with Federal guidelines.

3.9.2 Temporary access will only be granted during exceptional circumstances when official functions are performed, including meeting mission readiness requirements.

3.9.3 Temporary access will remain valid until the exceptional circumstances have abated, the access is no longer needed, the access is terminated, and/or the final eligibility is granted.

3.9.4 Temporary access will not exceed one year unless approved by the AA, OPS, or designee. Justification for approved temporary access exceeding one year will be recorded and maintained by the granting agency.

3.9.5 Temporary access will only be granted to U.S. citizens.

3.9.6 The NASA CAF shall maintain all records related to temporary access.

3.10 Access to Restricted Data (RD) or Formerly Restricted Data (FRD)

3.10.1 Access to RD and FRD requires clearance by the Department of Energy (DOE) or the Nuclear Regulatory Commission (NRC).

3.10.2 If such access is required solely for the performance of service for another agency, that agency will initiate the required investigation. The NASA CAF shall assist the other agency in obtaining and providing the required security documents.

3.10.3 When access to RD or FRD is required in the performance of NASA duties, a request for DOE access will be submitted in IdMAX and processed by the NASA CAF.

3.10.4 The NASA CAF shall report the granting of access to RD and FRD to the DSMD and the RD Management Official.

Appendix A. Definitions

Access - The explicit granting of permission to enter and/or use facilities, interact with personnel, and/or use information and related information processing services.

Adjudication - A fair and logical determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual's suitability for employment, fitness to perform work, and/or eligibility for access are in the best interests of the U.S. Government.

Adjudicative System of Record - Previously referred to as the Clearance Verification System or CVS, the official system(s) for maintaining records of all adjudicative actions.

Applicant - An individual undergoing vetting through an investigative process.

Asset - A system, object, person, or any combination thereof that has importance or value; includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

Automated Record Checks - A centralized and integrated set of electronic services to request, collect, and validate electronically accessible, adjudicative-relevant data using the most efficient and cost-effective technology and methods available.

Center Chief of Protective Services (CCPS) - See definition for Center Chief of Security (CCS).

Center Chief of Security (CCS) - The senior Center security official who is responsible for management of the Center security program.

Central Adjudication Facility (CAF) - Facility established at the OPS Security Management Division level responsible for adjudicating all requests for clearances to access CNSI.

Certification - A formal process used by the certifying official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

Classified Material - Any physical object on which is recorded, or in which is embodied, CNSI that can be discerned by the study, analysis, observation, or other use of the object itself.

Classified National Security Information (CNSI) - Information that is protected against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Cohabitant - An individual with whom the applicant resides.

Component Facilities - NASA-owned facilities not located on any NASA Center (e.g., Michoud Assembly Facility, Wallops Flight Facility, and White Sands Test Facility).

Continuous Evaluation - Reviewing the background of an individual who is eligible for access to CNSI or who holds a sensitive position (including additional or new checks of commercial and Government databases and other lawfully available information) at any time to determine whether that individual continues to meet the requirements for eligibility for access to CNSI and/or to hold a sensitive position.

Contractor - For the purpose of this NPR, any non-NASA entity or individual working on a NASA installation or accessing NASA physical or logical resources for an employer who is subject to E.O.

11246.

Core Duty - A continuing responsibility that is of a particular importance to the relevant covered position or the achievement of an agency's mission.

Corroborate - Comparing information from any ISP with that provided by the subject to confirm the information or identify discrepancies.

Covered Individual - Any person who performs work for or on behalf of the executive branch or who seeks to perform work for or on behalf of the executive branch.

Credential - For the purposes of this policy, a smartcard (PIV or Agency Smart Badge) issued to an individual that contains stored biometric information so that the claimed identity of the cardholder can be verified against the stored information manually or by an automated process.

Critical Sensitive - One of the three levels for designating national security-related positions and the degree of risk involved. Includes any position involving access to Top Secret information.

Debarment - Official determination made in writing by the Center Director or Center Chief of Security that bars, for cause, an individual from accessing NASA property.

Denial - The adjudication that an individual's initial access to CNSI would pose a risk to national security, after review procedures set forth in E.O. 12968 have been exercised.

Determination - A decision by an agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency.

Employee - A NASA civil service employee or NASA contractor.

Enhanced Subject Interview - An in-depth discussion between a trained and certified investigator and the subject conducted as a required part of an investigation or to offer the subject an opportunity to explain, refute, or mitigate issue or discrepant information.

Excepted Service - Those positions: (a) not in the competitive service, (b) not in the Career Senior Executive Service, and (c) not in the intelligence community unless covered by OPM appointing authorities.

Executive Order (E.O.) - Official documents, numbered consecutively, through which the President of the United States manages the operation of the Federal Government.

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

Foreign National - For the purpose of this policy, any person who is not a citizen of the United States including lawful permanent resident (i.e., holders of green cards) or persons admitted with refugee status to the United States. See definition of Lawful Permanent Resident (LPR) in this chapter.

Formerly Restricted Data (FRD) - Information developed by the Department of Energy (DOE) related to national nuclear programs with strict access restrictions, "Restricted Data (RD)," but that has subsequently been downgraded to a lower level of control and accountability.

Immediate Family - The spouse, parents, siblings, children, and cohabitant of the subject. This

includes any stepparents, half siblings and stepsiblings, and stepchildren of the subject.

Intelligence Community - The aggregate of the following executive branch organizations and agencies involved in intelligence activities: the Central Intelligence Agency, the National Security Agency, the Defense Intelligence Agency, offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs, the Bureau of Intelligence and Research of the Department of State, intelligence elements of the military services, the Federal Bureau of Investigation, the Department of Homeland Security, the Department of the Treasury, the Department of Energy, and staff elements of the Office of the Director of Central Intelligence.

Intergovernmental Personnel Act (IPA) Employees - Individuals on temporary assignments between Federal agencies and state, local, and Indian Tribal Governments; institutions of higher education; and other eligible organizations.

Investigative Questionnaire System of Record - Previously the Electronic Questionnaires for Investigation Processing or e-QIP system, the official system(s) for maintaining records of all investigative information, including self-reporting biographic details, declarations, clarifications, and mitigating information necessary to conduct investigations.

Investigative Record - The official record of all data obtained on the subject from trusted information providers from suitability and/or security applications and questionnaires and any investigative activity conducted under Federal standards.

Lawful Permanent Resident (LPR) - A foreign national, legally permitted to reside and work within the U.S. who may be employed in the Federal sector for specific needs or under temporary appointments but who may not be granted access to CNSI. For more information, refer to NPR 1600.4.

Logical Access - Access to information records, data, systems, and applications.

NASA Worker - Persons who directly support the mission and goals of NASA and/or are compensated by NASA (e.g., Federal civil servants, contractors, grantees, interns, etc.).

Physical Access - Access to federally controlled facilities.

Position Designation - The assessment of the potential for adverse impact on the efficiency and integrity of the service and the degree to which, by the nature of the position, the occupant could bring about a material adverse effect on the national security.

Position Risk – The designation of the level of risk associated with a position based on the potential impact to the efficiency or integrity of the service and its effect on the Agency or on the Agency’s mission.

Position Sensitivity - The designation of the level of risk associated with a position based on the actual or potential access to CNSI and the degree of damage an individual in the position could affect national security.

Public Trust Position - Position at the high-risk or moderate-risk level 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 - The acceptance of an existing investigation and adjudicative decision, made by another Federal agency, to establish suitability, fitness, or eligibility.

Revocation - The removal of an individual's eligibility for access to CNSI and/or to hold a sensitive position based upon an adjudication that continued access poses an undue risk.

Risk Acceptance - An official acknowledgement by management officials that they accept the risk posed by not implementing a recommendation, or requirement, designed to reduce or mitigate a risk.

Risk Assessment - The process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.

Risk Management - A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

Security Violation - An act or action by an individual or individuals that is in conflict with NASA security policy or procedure, such as a loss of CNSI, refusal to properly display NASA photo identification, violation of escort policy, or security area violations. This does not include incidents of theft, assault, and other related criminal activity.

Senior Management Official - Agency or Center management personnel at Division Chief or higher level.

Sensitive Compartmented Information (SCI) - Classification level denoting information, generally intelligence related, requiring security eligibility and physical/procedural security measures above those established for collateral CNSI or Special Access Program (SAP) information.

Sensitive Positions - Positions that have the potential to cause damage to national security. These positions require access to CNSI and are designated by the level of potential damage to national security:

- a. **Confidential** - Information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security.
- b. **Secret** - Information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to national security.
- c. **Top Secret** - Information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security.

Special Access Program (SAP) - Any program established and approved under E.O. 12958 that imposes need-to-know or access controls beyond those normally required for access to collateral Confidential, Secret, or Top Secret information.

Suitability - An assessment of an individual's character or conduct that may have an impact on promoting the efficiency and integrity of the Federal service.

Suspension - The temporary removal of an individual's access to CNSI.

Trusted Information Provider - An authorized individual working for or on behalf of the Government who may contact references or otherwise corroborates or verifies subject data, such as

citizenship, education, and former employment. These individuals may include Government and contract employees or military personnel working in human resources or security offices, or equivalent organizations.

Unauthorized Disclosure - A communication or physical transfer of CNSI to a recipient who does not have the required credentials for access.

Verification - Validating at the actual source (an individual or place of record - such as employers, courts, law enforcement agencies - or their authorized repositories) the correctness and accuracy of information listed in the investigative questionnaire system of record or provided by the subject or references to the trusted information provider.

Appendix B. Acronyms

AA	Assistant Administrator
CAF	Central Adjudication Facility
CARP	Credentialing/Fitness Adjudication Review Panel
CCPS	Center Chief of Protective Services
CCS	Center Chief of Security
CFR	Code of Federal Regulations
CO	Contracting Officer
COR	Contracting Officer's Representative
CNSI	Classified National Security Information
DOD	Department of Defense
DOE	Department of Energy
DSMD	Director, Security Management Division
EO	Executive Order
FRD	Formerly Restricted Data
HSPD	Homeland Security Presidential Directive
IdMAX	Identity Management and Account Exchange
IPA	Intergovernmental Personnel Act
ISP	Investigative Service Provider
LOI	Letter of Intent
LON	Letter of Notice
LPR	Lawful Permanent Resident
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NASA	National Aeronautics and Space Administration
NCHC	National Criminal History Check
NCIC	National Crime Information Center (DOJ)
NISPOM	National Industrial Security Program Operating Manual
NMO	NASA Management Office
NPD	NASA Policy Directive
NRC	Nuclear Regulatory Commission

NPR	NASA Procedural Requirement
OCHCO	Office of the Chief Human Capital Officer
OGC	Office of General Counsel
ODNI	Office of the Director of National Intelligence
OIG	Office of the Inspector General
OIIR	Office of International and Interagency Relations
OPM	Office of Personnel Management
OPS	Office of Protective Services
PIV	Personal Identity Verification
PPD	Presidential Policy Directive
PSI	Personnel Security Investigation (formerly Background Investigation)
RD	Restricted Data
SAP	Special Access Program
SARP	Security Adjudication Review Panel
SCI	Sensitive Compartmented Information
SEAD	Security Executive Agent Directive
SMD	Security Management Division
TS	Top Secret
U.S.	United States
U.S.C.	United States Code

Appendix C. References

- C.1. Unlawful Acts: Lautenberg Amendment, 18 U.S.C. § 922 (g) (9).
- C.2. Security Clearances: Limitations, 50 U.S.C. § 435c (b).
- C.3. Suspension and Removal, 5 U.S.C. § 7532.
- C.4. e-Gov Act of 2002, Pub. L. No. 107-347.
- C.5. Crime Control Act of 1990, Child Care Worker Employee Background Checks, Pub. L. 101-647 (1990).
- C.6. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (2004).
- C.7. Security Requirements for Government Employment (1953), E.O. 10450.
- C.8. Drug-free Federal Workplace (1986), E.O. 12564.
- C.9. Reforming Processes Related to Suitability for Government Employment, fitness for contractor employees, and eligibility for Access to Classified National Security Information (2008), E.O. 13467.
- C.10. Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Position of Trust (2009), E.O. 13488.
- C.11. Classified National Security Information (2009), E.O. 13526.
- C.12. Amending the Civil Service Rules, Executive Order 13488 and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters (2017), E.O. 13764.
- C.13. National Security Positions, 5 CFR pt. 1400.
- C.14. National Security Information, 32 CFR pt. 2003.
- C.15. NPD 1440.6, NASA Records Management.
- C.16. NPD 1600.9, NASA Insider Threat Program.
- C.17. NPR 1382.1, NASA Privacy Procedural Requirements.
- C.18. NPR 2810.1, Security of Information Technology.
- C.19. Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004).
- C.20. Memorandum for Heads of Agencies Aligning OPM Investigative Levels with Reform Concepts (August 24, 2010).
- C.21. OMB Memorandum M-05-24, Memorandum for the Heads of All Departments and Agencies, Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors (August 5, 2005).

- C.22. OMB Memorandum M-11-11, Memorandum for the Heads of Executive Departments and Agencies, Continued Implementation of Homeland Security Presidential Directive (HSPD) - 12, Policy for a Common Identification Standard for Federal Employees and Contractors (February 3, 2011).
- C.23. OMB Memorandum for Deputies of Executive Department and Agencies Reciprocal Recognition of Existing Personnel Security Clearances (July 17, 2008).
- C.24. OPM Federal Investigations Notice No. 10-05, Reminder to Agencies of the Standards for Issuing Credentials under HSPD-12 (May 17, 2010).
- C.25. OPM Memorandum, Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide (January 14, 2008).
- C.26. OPM Memorandum for Heads of Departments and Agencies, Final Credentialing Standards for Issuing Personal Identity Verification Cards Under HSPD-12 (July 31, 2008).
- C.27. White House Memorandum, Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information (December 29, 2005).
- C.28. Federal Information Processing Standards 201, Personnel Identity Verification (PIV) of Federal Employees and Contractors.
- C.29. Security Executive Agent, Suitability Executive Agent, Memorandum, Approval of Federal Investigative Standards (December 13, 2008).
- C.30. SEAD 5, Collection, use, and retention of publicly available social media information in personnel security background investigations and adjudications.
- C.31. SEAD 6, Continuous Evaluation.
- C.32. SEAD 7, Reciprocity of Background Investigations and National Security Adjudications.