**NASA NPR 1600.3B**

**Procedural** Effective Date: June 6, 2025

**Requirements** Expiration Date: June 6, 2030

**Subject: Personnel Security**

**Responsible Office: Office of Protective Services**

**Table of Contents**

[**Preface**](#_bookmark0)

* 1. [Purpose](#_bookmark1)
  2. [Applicability](#_bookmark2)
  3. [Authority](#_bookmark3)
  4. [Applicable Documents and Forms](#_bookmark4)
  5. [Measurement/Verification](#_bookmark5)
  6. [Cancellation](#_bookmark6)

[**Chapter 1. Introduction**](#_bookmark7)

* 1. [Overview](#_bookmark8)
  2. [Scope](#_bookmark9)
  3. [Roles and Responsibilities](#_bookmark10)
  4. [Violations of Security Requirements](#_bookmark11)

[**Chapter 2. Personnel Security Investigations and Adjudications**](#_bookmark12)

* 1. [General](#_bookmark13)
  2. [Risk and Sensitivity Levels](#_bookmark14)
  3. [Designation of Risk and Sensitivity Levels](#_bookmark15) for Investigations
  4. [Non-U.S. Citizens](#_bookmark16)
  5. [Childcare Providers](#_bookmark17)
  6. [Investigation Process Requirements](#_bookmark18)
  7. Trusted Workforce 2.0 and Continuous Vetting
  8. [Reciprocity of Investigations and Adjudications](#_bookmark19)
  9. [Adjudications](#_bookmark20)
  10. [Personnel Security File Storage and Access](#_bookmark21)

[**Chapter 3. Personnel Security for National Security Positions**](#_bookmark22)

* 1. [General](#_bookmark23)
  2. [Reciprocity of National Security Investigations and Adjudications](#_bookmark24)
  3. [Adjudication](#_bookmark25)
  4. [Suspension](#_bookmark26)
  5. [Denial or Revocation](#_bookmark27)
  6. [Continuous Evaluation](#_bookmark28)
  7. [Sensitive Compartmented Information (SCI)](#_bookmark29)
  8. [Temporary, Interim or One-Time Access to CNSI](#_bookmark30)

[**Appendix A. Definitions**](#_bookmark31)[**Appendix B. Acronyms**](#_bookmark32)[**Appendix C: References**](#_bookmark33)

# Preface

* 1. **Purpose**

1. This National Aeronautics and Space Administration (NASA) Procedural Requirement (NPR) establishes the Agency-wide personnel security program implementation requirements set forth in NASA Policy Directive (NPD) 1600.2, NASA Security Policy, as amended.
2. This NPR 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.

# Applicability

1. This NASA directive applies to NASA Headquarters and all NASA Centers, including Component Facilities and Technical and Service Support Centers.
2. This directive applies to the Jet Propulsion Laboratory, a Federally Funded Research and Development Center (FFRDC), only to the extent specified in the NASA/Caltech prime contract.
3. This directive is applicable to other contractors, recipients of grants and cooperative agreements, or parties to other agreements only to the extent specified or referenced in the applicable contracts, grants, or agreements.
4. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term “shall.” The term “may” denotes a discretionary privilege or permission, “can” denotes statements of possibility or capability, “should” denotes a good practice, and is recommended, but not required, “will” denotes an expected outcome, and “are/is” denotes descriptive material.
5. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

# Authority

1. National and Commercial Space Programs, 51 United States Code (U.S.C.) § 20132, Public Law (Pub.L.) 111-314, 124 Stat. 3328 (2010).
2. NPD 1600.2, NASA Security Policy.

# Applicable Documents and Forms

1. Freedom of Information Act, 5 U.S.C. 552.
2. Suspension and Removal, 5 U.S.C. § 7532.
3. NPR 1441.1, NASA Records Retention Schedules.
4. NPR 1600.2, NASA Classified National Security Information (CNSI).
5. NPR 1600.4, Identity and Credential Management.
6. NPR 3730.1, NASA Suitability Program.
7. Security Executive Agent Directive (SEAD)-7, Reciprocity of Background Investigations and National Security Adjudications.
8. Security Executive Agent Directive (SEAD)-8, Temporary Eligibility.
9. Security Executive Agent Directive (SEAD)-9, Whistleblower Protection: Appellate Review of Retaliation Regarding Security Clearances and Access Determinations.
10. DoD Manual 5220.22, Volume 2, National Industrial Security Program: Industrial Security Procedures for Government Activities, August 1, 2018.

# Measurement/Verification

a. Compliance with this NPR will be achieved by the Agency-wide application of uniform suitability, eligibility, contractor fitness, and adjudication procedures that foster reciprocity, reduce duplication of 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.

# Cancellation

a. NPR 1600.3A, Personnel Security, dated August 3, 2020.

# Chapter 1. Introduction

* 1. **Overview**
     1. This NASA directive establishes the policies and high-level procedures that are 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 to conduct business.
     2. Personnel security processes and practices encompass all activities necessary to investigate and adjudicate personnel security investigations, including position risk designations, reinvestigations, and continuous evaluations.
     3. Personnel security background investigations, also referred to as investigations, are used to evaluate the character and conduct of all NASA workers (civil service employees and contractors) 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, as appropriate.

# Scope

* + 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 encompasses all investigations and adjudications aimed at determining eligibility for access to non-sensitive and sensitive assets.
    2. NASA requirements for suitability are outlined in NPR 3730.1, NASA Suitability Program.

# Roles and Responsibilities

* + 1. The NASA Administrator shall implement a comprehensive and effective personnel security program for the Agency.
    2. The Assistant Administrator, Office of Protective Services (AA, OPS) shall:

1. 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, suitability and fitness policies, procedural requirements, and guidelines as established by the Defense Counterintelligence and Security Agency (DCSA), the Office of the Director of National Intelligence (ODNI), and the Office of Personnel Management (OPM).
2. Serve as the Agency Advocate for the investigative and adjudicative systems of record.
   * 1. The Director, OPS Personnel Security Division (PSD) shall:
3. Serve as the Agency Administrator and primary point of contact to DCSA, ODNI, and OPM.
4. Execute the personnel security program established by the AA, OPS.
5. Oversee the suitability determinations for first-time NASA civil service employees occupying a sensitive position.
6. Oversee the fitness determinations of all NASA contractors.
7. Oversee the physical and logical access eligibility determinations of all NASA workers.
8. Manage and oversee the Agency’s capability for determining eligibility for access to CNSI and/or to occupy a sensitive position.
9. Review and assess compliance with personnel security requirements for the Agency.
10. Ensure adjudications for credentialing are only performed by personnel security specialists who are trained and certified in accordance with Federal adjudication training standards.
    * 1. The Office of the Chief Human Capital Officer (OCHCO) shall:
11. Establish policies and oversee activities related to determining position risk and sensitivity for all NASA civil service employees.
12. Establish policies and oversee activities related to determining suitability for NASA civil service employees occupying non-sensitive positions.
13. Cooperate with security officials during security inquiries and investigations pertaining to the requirements of this policy.
    * 1. Personnel Security Specialists shall:
14. Process and submit all background investigation requests electronically using the investigative questionnaire system of record.
15. Ensure that a check of all required investigative and adjudicative systems of record is performed to validate any prior investigation or adjudication that will meet reciprocity standards before initiating a background investigation.
16. Maintain close coordination with the Investigative Service Provider (ISP) and process the appropriate requests for background investigations.
17. Perform adjudications of investigations to determine eligibility for credentialing, fitness, suitability, or national security.
18. Notify the Director, PSD, or designee, of any adverse information regarding any NASA employee at the Center that has access to CNSI or occupies a sensitive position.
19. Recommend suspension of a NASA civil service employee’s eligibility for access to CNSI and/or to hold a sensitive position based on developed disqualifying adverse information as detailed in this NPR.
20. Monitor, through continuous vetting, all NASA civil service employees with access to CNSI to ensure that personnel security requirements and policies for continued access are followed.
21. In cooperation with OCHCO, determine the risk and sensitivity of all positions requiring eligibility for access to CNSI.
22. Process requests for eligibility for access to CNSI or to occupy a sensitive position.
23. Refer all developed adverse information for NASA civil service employees to the appropriate OCHCO personnel for review.
24. Conduct National Criminal History Checks (NCHC) and other local records checks or automated record checks, as appropriate.
25. 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.
26. Maintain, in accordance with the Privacy Act, Pub. L. No. 93-579 and the existing NASA system of records, individual personnel security files on all investigated personnel.
27. Review applicable reports with officials in the review process who make determinations regarding continued access or revocation of access privileges.
28. Inform all investigated personnel of their rights to request under the Freedom of Information Act 5 U.S.C. 552 or, as applicable, any documents, records, and reports upon which an investigation was conducted.
    * 1. Managers and supervisors shall ensure full compliance with the requirements established in this policy and the OCHCO policy for suitability.
      2. The NASA General Counsel shall provide legal counsel as required within this policy.
      3. Contract Management Officials (Contractor Management, Contracting Officer, Contracting Officer’s Representative (COR), and Project Managers) shall:
29. Ensure full compliance with the requirements established in this policy.
30. Coordinate as needed with the PSD for the designation of risk and sensitivity, as well as the onboarding of contractor employees.
31. Make necessary notifications to contract management upon suspension or removal of contractor employees whose eligibility for access or the issuance of a NASA credential has been denied or revoked.

# Violations of Personnel Security Program Requirements

* + 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 possible prosecution under Violation of Regulations of National Aeronautics and Space Administration, 18 U.S.C. § 799, that provides fines or imprisonment for not more than 1 year, or both.

# Chapter 2. Personnel Security Background Investigations and Adjudications

* 1. **General**
     1. Individuals who perform work for or on behalf of the Agency shall be assigned to a position which has been designated in accordance with OPM position designation requirements.
     2. Individuals who perform work for or on behalf of the Agency are subject to a background investigation, in accordance with their assigned position, to determine whether they are:

1. Suitable for Government employment.
2. Eligible for logical and physical access.
3. Eligible for access to CNSI.
4. Eligible to hold a sensitive position.
5. Fit to perform work for or on behalf of the Government as a contractor employee.
   * 1. 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 employees 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 employees, in accordance with this policy and NPR 3730.1.
     2. All information obtained regarding personnel security reports and/or records will be handled in accordance with Pub. L. No. 93-579
     3. Intergovernmental Personnel Act (IPA) personnel will be adjudicated for access based on their position designation.
     4. NASA will reciprocate prior favorable suitability, fitness, and national security determinations for that investigation tier and lower investigation tiers in compliance with the requirements for reciprocity found in this policy and NPR 3730.1.
     5. An individual who requires a higher level of investigation will be subject to a new investigation commensurate with the requirements of the higher-level investigation.
     6. All persons with a background investigation will be continuously evaluated to ensure continued suitability/fitness and/or eligibility.
     7. NASA will process all investigations using approved Federal Government systems, in compliance with policies for the use of these systems.
     8. The Identity Management and Account Exchange (IdMAX) system will be the authoritative system for tracking, initiating, and adjudicating investigations.
     9. IdMAX will be the authoritative system for designating contractor positions. Position designations for NASA civil service employees are maintained by OCHCO.

# Risk and Sensitivity Levels for Investigations

* + 1. Position risk will be designated as “Low-Risk,” “Moderate-Risk,” or “High-Risk.”
    2. Positions designated as “Moderate-Risk” or “High-Risk” will be referred to as “Public Trust” positions.
    3. Position sensitivity levels will be designated as “Non-Sensitive” or, for national security positions, as “Non-Critical Sensitive,” “Critical-Sensitive,” or “Special-Sensitive.”
    4. The appropriate level of background investigation will be initiated, as determined by both position risk and sensitivity levels, in accordance with the Federal Investigative Standards prescribed by the Office of Personnel Management and the Office of the Director, National Intelligence.

# Designation of Risk and Sensitivity Levels

* + 1. All position risk and sensitivity level designations will be made using the approved Federal Government position risk designation tool.
    2. OCHCO will assign position risk and sensitivity level designations to civil service employees in coordination with their supervisor and PSD.
    3. Position risk 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 COR; typically, by the designated civil service project manager (sponsor), in coordination with OPS, and Information Technology Security Manager(s) and in compliance with position designation standards.
    4. Position sensitivity level designations for national security contracts will be made in accordance with NPR 1600.2, NASA Classified National Security Information (CNSI).
    5. The position risk and sensitivity level for contractor positions will be identified and specified in the contract statement of work.
    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.
       1. The COR, in consultation with the contracting officer, is required to identify contract employees to be processed at each position 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. An entire contract, grant, Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU) may be designated as high or moderate risk; however, those NASA contractor employees whose work would be considered moderate or low risk will be investigated according to the highest-risk level associated with their duties. To address this contingency, the contract, grant, Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU) will include specific controls to ensure that the work of lower-risk positions does not overlap with that of higher-risk positions.

# Non-U.S. Citizens

* + 1. Non-U.S. (United States) citizens, including Lawful Permanent Residents (LPR), are eligible for placement in low-risk and moderate-risk positions, but are generally not eligible for employment in positions designated as high-risk, in accordance with NPR 1600.4. Appointments to high-risk positions will be made in accordance with the requirements of NPR 3300.1.
    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 moderate or high-risk position.

# Childcare Providers

* + 1. PSD will ensure that a minimum of a Tier 1 investigation shall be completed on all childcare providers before they work in NASA-sponsored childcare facilities. The appropriate extra coverage code, in accordance with Federal Personnel Investigative Vetting Standards, will be requested during the initiation of the investigation for childcare providers.

# Investigation Process Requirements

* + 1. An investigation will be initiated for all NASA workers, commensurate with the risk and sensitivity of their position.
    2. The applicant shall submit fingerprints through the IdMAX system.
    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.
    4. Investigation forms will be certified and submitted to the ISP within 14 days of the applicant’s signature.
    5. If the required investigation is determined not to have been accomplished at any time, the appropriate investigation will be conducted.
    6. At the discretion of OPS/PSD, 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.
    7. Changes in Position, Risk, or Sensitivity Level
       1. When a NASA worker experiences a change in work duties that increases the risk or sensitivity level, a new investigation commensurate with the risk or sensitivity will be transmitted to the ISP.
       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.

# Trusted Workforce 2.0 and Continuous Vetting

* + 1. In accordance with the January 2021 Executive Correspondence issued jointly by ODNI and OPM regarding implementation of Federal Personnel Investigative Vetting Standards and Trusted Workforce (TW) 2.0, reinvestigations for Tiers 2 through 5 will no longer be required once fully implemented. All individuals who have undergone a background investigation will be enrolled in an approved Continuous Vetting (CV) program. Reinvestigations will not be performed unless results from the CV necessitate an updated investigation. OPS/PSD will follow the TW 2.0 implementation strategies, requirements, and timelines outlined in various supporting documents published by ODNI and OPM. OPS/PSD will monitor additional TW 2.0 policy updates and timelines as they become available and will implement them accordingly.

# Reciprocity of Investigations and Adjudications

* + 1. Investigations completed by or on behalf of another Agency that meet the requirements for a specified position will be reciprocally accepted for that and lower investigations with no additional investigation provided there is no break in employment (in accordance with Federal guidelines), derogatory or questionable information post favorable adjudication, or need based on change of position with a higher investigation requirement.
    2. All investigative and adjudicative systems of record will be checked by a NASA personnel security specialist who has undergone a favorably adjudicated background investigation and received the required training to determine if a prior investigation or adjudication will serve reciprocally for a NASA determination of suitability, fitness, or access to physical and logical assets. If no favorably adjudicated background investigation is identified in an adjudicative system of record or any other trusted Government agency that will serve reciprocally, a background investigation will be initiated in the investigative questionnaire system of record, commensurate with the position’s risk and sensitivity.
    3. Reciprocal recognition will be granted for a prior favorable suitability, fitness, or access determination when:

1. Equivalent to Suitability, 5 CFR pt. 731 adjudicative criteria were used; and
2. The individual has had no break in employment more significant than 24 months since the favorable determination was made; and
3. The new position requires the same or a lower level of investigation than previously conducted for that individual; and
4. No developed adverse information has been obtained on the individual; and
5. The individual’s investigative record does not reflect conduct that is incompatible with the core duties of the new position; and
6. The investigation is within the same scope.

# Adjudications

* + 1. Trained and certified adjudicators will perform adjudications in accordance with Federal guidelines for credentialing, suitability, fitness, and eligibility for access to CNSI and/or to hold a sensitive position.
    2. Adjudicative decisions will be made on individuals for whom an appropriate investigation has been completed.
    3. Adjudicative decisions will be made in accordance with the appropriate Federal adjudicative standards.
    4. Adjudications will be performed within the established timelines identified in Federal guidelines and recorded in IdMAX and other required Government systems of record for recording adjudications.
    5. Adverse Information.
       1. When adverse information is developed or received in the course of any personnel security investigation, after such investigation and initial favorable determination, or through continuous vetting, the scope of inquiry will be expanded to the extent necessary to obtain sufficient determination and information to make a reasonable and sound determination to obtain or maintain suitability, fitness, or eligibility for access.
       2. When necessary, expanded inquiries or personal interviews will be conducted by a NASA official with appropriate investigative experience, NASA-contracted investigators, an appropriate investigating agency, or another Federal Government agency at NASA’s request.
          1. Appropriate signed releases from the employee will be obtained when required to pursue additional leads, such as medical records or credit checks.
       3. Counterintelligence-related adverse information will be relayed as soon as possible, but no later than the next business day after the information has been obtained, to OPS Counterintelligence and Counterterrorism.
       4. An adjudicator will 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 background investigation, database query, and adjudication. Adverse information involving civil service employees will be referred to OCHCO for appropriate action.
    6. Revocation of Eligibility for the Issuance of a NASA credential.

1. When an adjudicator determines removal of a non-NASA employee is warranted, in accordance with Federal adjudicative guidelines, they shall notify the Director, PSD, with the Adjudicative Summary and draft Letter of Revocation (LOR) for concurrence/signature.
2. The Director, PSD, will provide non-NASA employees with written notification of the reason(s) for revocation of access and the procedures and timeline (within 30 days of receipt of the letter) for submitting an appeal to the OPS Director, Field Operations. Should the individual elect not to appeal within 30 calendar days, as outlined in the LOR, or their employment on a NASA contract is terminated, the original revocation decision will be final, and there will be no further appeals.
3. If the non-NASA employee whose logical and physical access was revoked submits a timely appeal, the OPS Director, Field Operations, will review the information provided to determine whether the issues were mitigated or not mitigated, in accordance with Federal adjudicative guidelines. The Director of Field Operations (DFO) will provide the non-NASA employee with a written decision, either reinstating access eligibility or upholding the initial decision to revoke access. If the original decision is upheld, the appeal process is concluded.
4. Two years from the date of the decision by the DFO, OPS, the non-NASA employee is eligible to reapply for a NASA credential if employed on a contract requiring logical and/or physical access to NASA assets.

# Personnel Security File Storage and Access

* + 1. Records and information related to this policy will be managed in accordance with NPR 1441.1, NASA Records Management Program Requirements. Personnel security files are temporary records and will be destroyed in accordance with the disposition instructions in NPR 1441.1.
    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, and in compliance with the Privacy Act of 1974.
    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 5

U.S.C. 552 and Pub. L. No 93-579 procedures. The subject may be directed to make such requests directly from the Investigative Service Provider.

* + 1. The results of background investigations will be used by NASA for the limited purpose of making suitability, fitness, and/or eligibility determinations.
    2. Adjudicative determinations will be reported using the appropriate system.
    3. NASA Personnel Security Specialists shall only access background investigations and adjudicative records relevant to the specific individual for whom a hiring, credentialing, or eligibility determination is required. Background investigations and adjudicative records may be accessed at the direction of the Director

of PSD or their designee. Background investigations and adjudicative records will be accessed only through the designated systems.

* + 1. All records related to background investigations, database checks, screening records, adjudicative decisions, or similar personnel security files will be maintained securely in accordance with all applicable regulations, policies, and procedures.

# Chapter 3. Personnel Security for Sensitive Positions

* 1. **General**
     1. The purpose of the personnel security program for sensitive positions is to ensure that only loyal, trustworthy, and reliable people are granted access to Classified National Security Information (CNSI) or assigned to sensitive positions.
     2. All NASA civil service employees occupying a sensitive position will be investigated and adjudicated for eligibility to hold a sensitive position, consistent with appropriate Federal requirements.
     3. All NASA civil service employees requiring initial or continuing access to CNSI will be investigated and adjudicated for eligibility to access CNSI, consistent with appropriate Federal requirements.
     4. NASA contracts requiring access to CNSI will be processed in accordance with NPR 1600.2 and the requirements of National Industrial Security Program, Executive Order 12829, the Operating Manual (NISPOM), and NISPOM Supplement.
     5. Foreign nationals requiring access to CNSI will be processed in accordance with NPR 1600.2 and the requirements of Department of Defense Manual 5220.22, Volume 2, National Industrial Security Program: Industrial Security Procedures for Government Activities.
     6. All NASA civil service employees requiring access to Sensitive Compartmented Information (SCI) will be processed in accordance with this policy and NPR 1600.2.
     7. OPS shall implement an annual revalidation of access to CNSI, whereby personnel who have not required access to 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.
     8. No individual will be given access to CNSI or assigned to a sensitive position unless a favorable eligibility determination has been made.
     9. The OPS/PSD, in coordination with Center OPS personnel, supervisors, and OCHCO, shall make employment suitability determinations for individuals entering the Federal workforce and holding a sensitive position.
     10. Subjects of adjudications will be notified when an interim or final eligibility decision has been made, or reciprocity of an existing adjudication has been accepted.
     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.
     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.).
     13. The policies and procedures for suspension, denial, and revocation will not be confused with the procedures for the removal of an employee on national security grounds as outlined in Suspension and Removal, 5 U.S.C. § 7532. OPS/PSD will coordinate with OCHCO to pursue the removal of a NASA civil service employee on national security grounds regardless of the employee’s position sensitivity or access to CNSI.

# Reciprocity of National Security Investigations and Adjudications

* + 1. Reciprocity will follow the requirements established in section [2.8,](#_bookmark19) [Reciprocity of Investigations and](#_bookmark19) [Adjudications.](#_bookmark19)
    2. Reciprocity will be granted in accordance with SEAD-7, Reciprocity of Background Investigations and National Security Adjudications.

# Adjudication

* + 1. Adjudications will follow all relevant Federal policies and regulations, including but not limited to, Security Executive Agent Directive (SEAD) 4, National Security Adjudicative Guidelines, and the Bond Amendment.
    2. Adjudications will be fully documented and recorded in the subject’s security file and entered into the appropriate adjudicative system of record.
    3. All reasonable efforts will be pursued to develop potential issue information, as well as potentially favorable or mitigating information.
    4. Adjudications will be made by certified national security adjudicators in accordance with National Security Adjudication Standards.
    5. Adjudications for first-time access will be performed on closed investigations commensurate with the required access.
    6. Adjudications will be continuously evaluated against all new information obtained after the initial national security adjudication and in compliance with Federal standards.

# Suspension

* + 1. The AA, OPS, or designee shall make all suspension determinations.
    2. The OPS Center Chief of Protective Services shall propose suspensions of security clearances to the Director, PSD, for cause based on developed adverse information.
    3. The AA, OPS, or designee shall make a final determination after consultation with the Director, PSD, and Office of General Counsel (OGC) personnel.
    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.
    5. The Director, PSD, will notify the NASA civil service employee in writing of the suspension. The reason or reasons for a suspension need not be provided to the subject of a suspension.
    6. Suspensions should not be open-ended. Every effort should be made to complete subsequent investigations and adjudications as soon as practical. All suspension actions should be resolved as soon as possible from the date of the suspension, if possible.
    7. Suspension of an individual’s access to CNSI will allow the Agency sufficient time to investigate and adjudicate information that may affect the individual’s eligibility for access to CNSI.
    8. The subject of a suspension shall not be entitled to review procedures.
    9. The Director, PSD, 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 the section [3.5,](#_bookmark27) [Denial or Revocation.](#_bookmark27)

# Denial or Revocation

* + 1. In the event of a denial or revocation, the NASA civil service employee is entitled to obtain a review of the decision.
    2. Only the AA, OPS, or designee shall make a denial or revocation determination.
    3. In the event of an unfavorable adjudication action, the Director, PSD, or designee 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.
    4. The Director, PSD, shall review the proposed unfavorable adjudicative action by the Adjudicator and:

1. Remand the case for further work; or
2. Uphold the proposed adjudication of the information, and in consultation with the Office of General Counsel (OGC), provide written notice to the subject of the denial or revocation through a PSD designee.
   * 1. The NASA civil service 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 Adjudicator will review the latest information provided. The Adjudicator will make a recommendation to the Director, PSD, 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 Adjudicator will continue with the denial or revocation process. Upon completion of the process, the employee will be notified by the Director, PSD, of a final decision in a Letter of Notification (LON). The letter is served through the PSD designee.
     2. The NASA civil service employee will be allowed to appeal the initial determination by the Director, PSD, to the AA, OPS, within the timeframe specified in the LON. The employee may submit the appeal in writing or request an in-person or virtual hearing with 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, will ensure that the subject’s rights are protected and that due process is accorded. The AA, OPS, will document all due process actions through a written summary, recording, or similar record, which will be included in the subject’s security record.
     3. 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 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 be assigned to a favorable Tier 5, and only one panel member may be a security professional. If the 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 choose to appeal in person to the SARP. Any personal appearance before the SARP will be documented in a recording, which will be included in the subject’s security record.
     4. Before finalizing the SARP determination, a SARP panel member or the AA, OPS, may refer the SARP proposed decision to the Administrator for an additional level of review. If no referral is made to the Administrator, the SARP decision is final. If a referral is made to the Administrator, the Administrator’s decision constitutes the final Agency decision.
     5. If a NASA civil service employee subject to a denial or revocation action related to eligibility for access to CNSI and/or to hold a sensitive position (including having received an LOI or LON) believes the determination was made in retaliation for making a protected disclosure, or for participating in same (such as a witness), as defined within SEAD 9, Whistleblower Protection: Appellate Review of Retaliation Regarding Security Clearances and Access Determinations, they may, at any point, submit a complaint to the NASA Office of Inspector General (OIG) Hotline or the local NASA OIG office for review. An employee alleging reprisal who has exhausted the internal NASA appeal process, including review by the NASA OIG, may request an external review in accordance with SEAD 9. The NASA Administrator shall carefully consider the findings and recommendations of any external review panel. Where these reviews are requested, in his/her sole discretion, the AA, OPS, may await the review of the employee’s case before deciding, or may take action to 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 understanding that the employee may be reinstated and compensated for damage due to an improper denial, suspension, or revocation of eligibility for access to CNSI and/or to hold a sensitive position. Any report provided will be carefully 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.
     6. Upon determination that a revocation or denial has been upheld, the case will be referred to OCHCO.

# Continuous Vetting

* + 1. All cleared individuals will be subject to a continuous vetting of their qualifications to meet the high standards of conduct expected of persons in sensitive positions.
    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. The PSD shall conduct fact-finding of reports of disqualifying conduct. Depending on the adverse impact on 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 background investigation may be requested to support the evaluation of an employee’s continued eligibility for access to CNSI and/or to occupy a sensitive position. The PSD will determine if the individual continues to be eligible for access to CNSI and/or to occupy a sensitive position.
    4. Foreign travel and contacts, both official and unofficial, will be reported and tracked in accordance with NPR 1600.2.
    5. Foreign travel and contacts, both official and unofficial, will be reviewed by the PSD as part of the continuous evaluation program.
    6. Information developed during the continuous vetting 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 will otherwise be ineligible for or lose continuation of Federal employment.

# Sensitive Compartmented Information (SCI)

* + 1. Candidates for access to SCI will occupy a position designated as special-sensitive.
    2. Candidates for access to SCI will have a favorably adjudicated investigation for a Top Secret (TS) clearance and be briefed.
    3. OPS shall manage and submit to the Cognizant Security Authority (CSA) all information necessary to determine eligibility for access to SCI.
    4. Upon the CSA granting SCI eligibility, OPS will ensure the candidate is briefed.

# Temporary/Interim or One-Time Access to CNSI

* + 1. Temporary, interim, or one-time access determinations will only be granted by the PSD in accordance with SEAD 8, Temporary Eligibility.
    2. The PSD shall maintain all records related to one-time or temporary/interim access determinations in accordance with SEAD 8.

# 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.

Adjudicator – A NASA Personnel Security Specialist trained and certified to review and adjudicate background investigations for credentialing, fitness, suitability, or national security access.

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

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 will be discerned by the study, analysis, observation, or other use of the object itself.

Classified National Security Information – Any physical object on which is recorded, or in which is embodied, CNSI that shall 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 Vetting – 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. Continuous Vetting (CV) is also a process that involves regularly reviewing a cleared individual’s background to ensure they continue to meet requirements for access to Federal facilities, IT assets, and the issuance of a credential.

Contractor – For 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 Executive Order 11246.

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

Credential – For 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; investigative requirements for this position are covered under National Security Directive 61.

Defense Counterintelligence and Security Agency – A Department of Defense agency that provides industrial security, personnel security, counterintelligence, insider threat, and security training support for the Federal Government.

Denial – The adjudication that an individual’s initial access to CNSI would pose a risk to national security, after review procedures outlined in Access to Classified Information, Executive Order 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.

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 – 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 this policy, any person who is not a citizen of the United States, including lawful permanent residents (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.

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 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 per 5 CFR, Part 7, Section 7.4, but who may not be granted access to CNSI.

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, etc.).

OPS Center Chief of Protective Services (CCPS) – See definition for Center Chief of Security (CCS). Physical Access – Access to Federally controlled facilities.

Position Risk 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 Sensitivity – The designation of the level of risk associated with a position based on the actual or possible access to CNSI.

Public Trust Positions – Positions at the high-risk or moderate-risk level are typically designated as public trust positions. Such positions may involve policy-making, significant program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties that demand a substantial degree of public trust, and positions involving access to, or operation or control of, financial records with a considerable risk of 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 NASA facilities, IT systems, or the issuance of a credential based upon an adjudication that continued access poses an undue risk.

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:

* Confidential – Information, the unauthorized disclosure of which reasonably could be expected to cause damage to national security.
* Secret – Information, the unauthorized disclosure of which reasonably could be expected to cause severe damage to national security.
* 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 Executive Order 12958 that imposes need-to-know or access controls beyond those typically 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 corroborate or verify subject data, such as citizenship, education, and former employment. These individuals may include Government and contract employees, as well as 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 appropriate credentials for access.

# Appendix B. Acronyms

|  |  |
| --- | --- |
| AA | Assistant Administrator |
| CCPS | Center Chief of Protective Services |
| CFR | Code of Federal Regulations |
| COR | Contracting Officer’s Representative |
| CNSI | Classified National Security Information |
| CSA | Cognizant Security Authority |
| CV | Continuous Vetting |
| DCSA | Defense Counterintelligence and Security Agency |
| DFO | Director of Field Operations |
| DOE | Department of Energy |
| FRD | Formerly Restricted Data |
| HSPD | Homeland Security Presidential Directive |
| IPA | Intergovernmental Personnel Act |
| IdMAX | Identity Management and Account Exchange |
| ISP | Investigative Service Provider |
| LOI | Letter of Intent |
| LON | Letter of Notice |
| LOR | Letter of Revocation |
| LPR | Lawful Permanent Resident |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| NASA | National Aeronautics and Space Administration |
| NBIS eAPP | National Background Investigations Services Electronic Application |
| NCHC | National Criminal History Check |
| NCIC | National Crime Information Center (DOJ) |
| NISPOM | National Industrial Security Program Operating Manual |
| NOJMO | NASA Office of JPL Management and Oversight |
| NPD | NASA Policy Directive |
| 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 |
| OPM | Office of Personnel Management |
| OPS | Office of Protective Services |
| PIV | Personal Identity Verification |
| PSD | Personnel Security Division |
| SAP | Special Access Program |
| SARP | Security Adjudication Review Panel |
| SCI | Sensitive Compartmented Information |
| SEAD | Security Executive Agent Directive |
| TS | Top Secret |
| TW | Trusted Workforce |
| U.S. | United States |
| U.S.C. | United States Code |

**Appendix C: References**

* 1. Violation of Regulations of National Aeronautics and Space Administration, 18 U.S.C. §799.
  2. Unlawful Acts, Lautenberg Amendment, 18 USC §922 (g) (9).
  3. Security Clearances; Limitations, 50 U.S.C. § 435c (b).
  4. e-Gov Act of 2002, Pub. L. No. 107-347, 44 U.S.C. Ch. 36.
  5. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (Dec 17, 2004).
  6. Crime Control Act of 1990, Childcare Worker Employee Background Checks, Pub. L. No. 101-647.
  7. Privacy Act of 1974, Pub. L. No. 93-579.
  8. Security Requirements for Government Employment, of April 17, 1953, as amended, E.O. 10450.
  9. National Industrial Security Program, of January 6, 1993, as amended, E.O. 12829.
  10. Access to Classified Information, of August 2, 1995, as amended, E.O. 12968.
  11. Reforming Processes Related to Suitability for Government Employment, fitness for contractor employees, and eligibility for Access to Classified National Security Information, of June 30, 2008, E.O. 13467.
  12. Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Position of Trust, of January 22, 2009, E.O. 13488.
  13. Classified National Security Information, of December 29, 2009, E.O. 13526.
  14. Suitability, 5 CFR pt. 731.
  15. Designation of National Security Positions, 5 CFR pt. 1400.
  16. National Security Information, 32 CFR pt. 2003.
  17. 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.
  18. 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.
  19. NPD 1440.6, NASA Records Management.
  20. NPD 1600.9 NASA Insider Threat Program.
  21. NPR 1382.1, NASA Privacy Procedural Requirements.
  22. NPR 2810.1, Security of Information and Information Systems.
  23. Joint ODNI/OPM Memorandum, Federal Investigative Standards, dated December 2012.
  24. Joint ODNI/OPM Memorandum, Transforming Federal Personnel Vetting: Continuous Vetting and Other Measures to Expedite Reform and Transition to Trusted Workforce 2.0, dated January 2021.
  25. Joint ODNI/OPM Memorandum, Trusted Workforce 2/0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers, dated March 2023.
  26. Federal Information Processing Standards 201-3, “Personnel Identity Verification (PIV) of Federal Employees and Contractors,” January 2022, as amended.
  27. Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors of August 27, 2004.
  28. Office of Personnel Management Memorandum “Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12,” July 31, 2008.
  29. Office of Personnel Management Memorandum “Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirements for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials,” December 15, 2020.
  30. Security Executive Agent Directive (SEAD)-3, Reporting Requirements.
  31. Security Executive Agent Directive (SEAD)-4, National Security Adjudicative Guidelines.
  32. Security Executive Agent Directive (SEAD)-5, Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications.
  33. Security Executive Agent Directive (SEAD)-6, Continuous Evaluation.