

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

NPD 1600.2E
 Effective Date: April 28, 2004
 Expiration Date: March 31, 2020

COMPLIANCE IS MANDATORY[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: NASA Security Policy (Revalidated on 4/2/2015 w/Change 1)**Responsible Office: Office of Protective Services**

Chg#	Date	Description/Comments
1	04/2/2015	Updated directive with administrative changes to comply with NPR 1400 new revisions. Also updated to reflect correct titles and numbers, removed canceled/deleted directives; updated P.2 section to comply with 1400.

1. POLICY

It is NASA's policy to provide security and protection for its personnel, including employees, authorized contractors, subcontractors, tenants, and visitors; its missions, facilities, property, and information that are in its possession or under its control, consistent with all applicable laws, national level directives, and Agency requirements.

2. APPLICABILITY

- a. This directive is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This directive applies to the Jet Propulsion Laboratory, a Federally Funded Research and Development Center, and other contractors only to the extent specified or referenced in the appropriate contracts.
- b. Nothing in this directive shall be considered to limit the authorities of the Office of the Inspector General under the Inspector General Act of 1978, as amended.
- 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, and "will" denotes expected outcome, and "are/is" denotes descriptive material.
- d. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

3. AUTHORITY

51 U.S.C. Sections 20133 & 20134 National and Commercial Space Program, as amended.

4. APPLICABLE DOCUMENTS AND FORMS

- a. 5 U.S.C. 7312, Employment and Clearance; Individuals Removed for National Security.
- b. 5 U.S.C. 7532, Suspension and Removal.
- c. 40 U.S.C. 1441 et seq., Computer Security Act of 1987.

- d. 42 U.S.C. 13041, Child Care Worker Employee Background Checks.
- e. 44 U.S.C. 3541 et seq., Federal Information Security Management Act (FISMA).
- f. 50 U.S.C. 401 et seq., Protection and Reduction of the Government Secrecy Act.
- g. 50 U.S.C. 435, National Security.
- h. EO 12829, as amended, National Industrial Security Program.
- i. EO 12958, Classified National Security Information, as amended by EO 13292.
- j. EO 12968, Access to Classified Information.
- k. 5 CFR Part 731, Suitability.
- l. 5 CFR Part 732, National Security Positions.
- m. 5 CFR Part 736, Personnel Investigations.
- n. 14 CFR Part 1203, Subpart H, Delegation of Authority to Make Determinations in Original Classification Matters.
- o. 14 CFR Part 1203a, NASA Security Areas.
- p. 14 CFR Part 1203b, Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel.
- q. 14 CFR Part 1204, Subpart 10, Inspection of Persons and Personal Effects on NASA Installations or on NASA Property; Trespass or Unauthorized Introduction of Weapons or Dangerous Materials.
- r. 32 CFR Part 2001, Classified National Security Information.
- s. OMB Circular No. A-130, Management of Federal Information Resources, (Appendix-III).
- t. NPR 1371.2, Procedural Requirements for Processing Requests for Access to NASA by Foreign Nationals or Representatives.
- u. NPD 1371.5, Accessing Foreign Nationals or Representatives to NASA Centers.
- v. NPR 1600.x, NASA COMSEC Procedural Requirements.
- w. NPR 1620.1, NASA Security Procedural Requirements.
- x. NPD 2190.1, NASA Export Control Program.
- y. NPR 2190.1, NASA Export Control Program.
- z. NPD 2810.1, Security of Information Technology.
- aa. NPD 9800.1, NASA Office of Inspector General Programs.
- bb. Security Policy Board (SPB) Issuance 1-97, Investigative Standards for Background Investigations for Access to Classified Information.
- cc. SPB Issuance 2-97, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.
- dd. National Security Directive 63, Single Scope Background Investigation.
- ee. Memorandum on Roles and Responsibilities of NASA's Office of Inspector General and Office of Security Management and Safeguards, dated December 10, 2003.

5. RESPONSIBILITY

- a. The Office of Protective Services (OPS), is responsible for:
 - (1) Establishing and maintaining a Foreign National Access Management (FNAM) program that enables the Office of Protective Services (OPS) to lead a partnership with the Office of the Chief Information Officer (OCIO) and the Office of International and Interagency Relations (OIIR) in the coordination and organization of all NASA Foreign National Management policies, procedures, and systems. Color-coded NASA photo-identification badge program or other state-of-the-art access controls means, including biometrics.
 - (2) Establishing and maintaining appropriate law enforcement and security operations, including investigations, through the development, implementation, and management of Federal Arrest Authority (FAA) and Use of Force policies, procedures, processes, standards, and training as necessary to ensure strict compliance with 14 CFR Part

1203b-Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel and 14 CFR Part 1204, Subpart 10, Inspection of Persons and Personal Effects on NASA Installations or on NASA Property; Trespass or Unauthorized Introduction of Weapons or Dangerous Materials.

(3) Establishing and maintaining appropriate relationships with federal, state, and local law enforcement agencies, including the NASA Office of the Inspector General, United States Attorney's Office, and local Office of the District Attorney, to ensure support and timely transfer of arrested persons and referral of criminal cases, as appropriate.

(4) Establishing and maintaining appropriate relationships with the national intelligence community for the purposes of obtaining and disseminating timely intelligence information, information on foreign intelligence collection efforts, and threat analysis.

(5) Establishing and maintaining an Insider Threat Program, which is intended to deter, detect, and mitigate insider threat actions by all employees, Federal and contractor. Integrate insider threat related policies, procedures and resources across NASA, such as security, counterintelligence, human capital, general counsel, information management and other authorities that contribute to deterring, identifying and managing insider threats.

(6) Establishing, in collaboration with the NASA Facilities Engineering Division, facility construction standards and guidelines that adequately address physical security and antiterrorism construction requirements and considerations.

(7) Ensuring that any person performing security functions for or on behalf of NASA at any NASA Center has been properly trained and certified to carry out such duties, has kept their qualifications current, and has had an appropriate favorable background investigation.

a. Developing, implementing, and maintaining appropriate and reasonable physical security controls at NASA Centers and facilities in accordance with Executive Order 12977, Interagency Security Committee, as amended by Executive Order 13286, Presidential Policy Decision 21, Critical Infrastructure and Resilience and Department of Homeland Security, Interagency Security Committee Standards, Establishing NASA Security Areas in accordance with 14 CFR 1203a.

b. Developing, implementing, and maintaining an Agency wide Enterprise Identity, Credential, and Access Management (ICAM) program utilizing Personal Identity Verification (PIV) Credentials, a Personal Identity Verification Card issuance program, and an integrated physical access control, video management, and intrusion detection system in accordance with the Federal Identity Credential and Access Management (FICAM) Roadmap, FIPS 201-2, OMB Memorandum M-11-11, and NIST Special Publication 800-116 and 800-79-1. In partnership with OCIO, ICAM is the sole provider of authoritative identity management and directory services, and the primary provider of credential and access management services (NPR 2841.1).

c. Reserving the right to search and briefly detain any person, including any property in the person's possession or control, as a condition of admission to, or continued presence on any NASA Center, or to deny entry, or remove from any NASA Center any person who refuses to comply with such conditions, consistent with applicable law.

d. Developing, implementing, and maintaining a robust Personnel Security Program for managing:

(1) Access to Classified National Security Information in accordance with Executive Order (EO) 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information and EO 13526, Classified National Security Information.

(2) Suitability for employment with NASA as established under 5 CFR Part 731 and EO 10450, Security Requirements for Government Employees, as amended.

(3) Appropriate security screening, in accordance with Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, and Federal Information Processing Standards (FIPS) 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors," and oversight of non-NASA civil service employees (e.g., contractors, grantees, foreign nationals, military detailees) requiring access to NASA Centers, Facilities, information, critical flight hardware and payloads, and information technology (IT) resources to ensure their continued reliability.

(4) Developing, implementing, and managing a security reporting and alerting system to provide timely notification of security threats and serious security incidents involving NASA Centers and/or personnel in accordance with Department of Homeland Security National Terrorism Advisory System.

(5) Undertaking a security education and awareness program designed to solicit the support and involvement of all its personnel.

(6) Imposing administrative review of all business related foreign travel by its employees when such review is appropriate in the interest of national security and personal safety of the individual(s) involved.

(7) Imposing appropriate access and movement controls on all visitors to NASA Centers in keeping with the purpose of the visit, availability of background investigative information, accesses required, and existing threats.

(8) Applying Department of Defense (DoD) Industrial Security Program standards to NASA classified contracts in accordance with Executive Order 12829, as amended by Executive Order 12885, National Industrial Security Program, DoD 5220,22-M, the National Industrial Security Program Operating Manual (NISPOM) and the NISPOM Supplement.

(9) Developing, implementing, and maintaining a classified National Security Information program which is managed in accordance with EO 13526, Classified National Security Information, and Information Security Oversight Office Directive Number 1, as amended.

(10) Developing, implementing, and maintaining appropriate contingency plans for the effective and timely transition to emergency and threat environments.

(11) Developing, implementing, and maintaining an Insider Threat Program that meets the requirements promulgated in EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, and the National Insider Threat Policy.

b. The Assistant Administrator (AA) for the Office of Protective Services (OPS), is responsible for the functional management and leadership for the overall development, implementation, and maintenance of the NASA Security Program, including:

(1) Developing and issuing, subject to coordination with and approval by the NASA General Counsel, security policy, procedures, and guidelines, in collaboration with Center Chiefs of Security (CCS), as appropriate.

(2) Denying, revoking, or suspending, in accordance with applicable processes, an Employee's security clearance in accordance with established requirements.

(3) In coordination with the Chief Information Officer (CIO), developing, implementing, and maintaining an Agency Identity, Credential, and Access Management Program designed to ensure appropriate controls for access to NASA facilities, information, information technology, and other resources.

(4) In coordination with the Chief Information Officer (CIO), developing, implementing, and maintaining an Agency communications security (COMSEC) and national security information systems within NASA, including accreditation of IT systems processing classified information, and serves as NASA's liaison with the National Security Agency, Department of Defense, and the intelligence community for processing national security information.

(5) In coordination with the Chief Information Officer (CIO) developing, implementing, and maintaining Agency-central Information Technology services supporting the operation of the Sensitive Compartmented Information and NASA Special Access Programs.

(6) Representing NASA as the point of contact with the national intelligence community and serving as the internal NASA point of contact for intelligence community information.

(7) Ensuring that FAA and Use of Force policies and procedures are consistently and uniformly managed throughout the Agency.

(8) Establishing appropriate relationships with the federal law enforcement community, including the NASA Office of the Inspector General and the Office of the General Counsel (OGC), to ensure proper management and referral of criminal cases and the timely transfer of arrested persons.

(9) Conducting periodic Functional Reviews of Protective Service activities at Centers and Component Facilities.

(10) Serve as NASA Senior Official in all matters relating to the NASA Insider Threat Program.

(11) Develops, implements, and maintains policy formulation, oversight, coordination and management of the Agency Protective Services, security services, counterintelligence (CI), counterterrorism (CT), emergency management planning, and continuity of operations functions.

b. Officials-in-Charge of Headquarters Offices are responsible for ensuring the implementation of this policy within their respective organization(s).

c. Center Directors are responsible for the following:

(1) Appointing, through coordination and concurrence by the AA for OPS, a qualified and experienced Center Chief of Security.

(2) Ensuring that local security procedures are established and managed that ensure the successful implementation of this policy and implementing NPR 1600.1, NASA Security Procedural Requirements.

(3) Keeping the AA for OPS informed of the threats directed against the Center, as well as the capabilities and limitations of the Center security program to counter such activities.

(4) Ensuring that security program self-assessments are conducted on schedule and in a forthright manner.

(5) Ensuring that physical access to NASA Centers is controlled through the utilization of a NASA Common Access Card (CAC), meeting the NASA CAC standards as prescribed in NPR 1600.1C, NASA Security Procedural Requirements, Chapter 7 and Appendix I, reference 4.a.

(6) Ensuring all allegations of actual or suspected espionage and terrorism threats are reported to the servicing NASA Counterintelligence/Counterterrorism office.

d. NASA Employees shall:

(1) Comply with NASA Security Policy and Procedural Requirements.

(2) Fully cooperate with security personnel during investigations or inquiries.

6. DELEGATION OF AUTHORITY

a. Center Directors may perform the following:

(1) Grant temporary security clearances to employees under their jurisdiction, subject to the eligibility standards set forth in Reference 4.a, as amended, and based on legitimate access requirements. This authority shall be redelegated to the Center Chief of Security.

(2) Suspend an employee's security clearance. Procedures for the suspension of NASA personnel security clearances are set forth in reference 4.a., as amended. This authority shall be redelegated to the Center Chief of Security.

b. The AA for OSPP is delegated the authority, under 42 U.S.C. Section 2456, to authorize such NASA employees, and contractor and subcontractor employees to carry firearms in the course of their duties when engaged in the protection of persons or property owned by the United States located at facilities owned or contracted to the United States.

This authority may be redelegated to the Center Chief of Security (CCS).

c. Authority is delegated to the officials designated below to make the determination and certification required by 42 U.S.C. Section 2455(b) for access by NASA representatives to Restricted Data in the possession of personnel of the Nuclear Regulatory Commission (NRC) and the Department of Energy and their contractors, and NRC and DoD cleared personnel of other Federal departments and agencies (except that access to Restricted Data within NASA and the DoD, based on a NASA or DoD clearance, is handled in the same manner as access to other classified information) and their contractors. The officials designated below may also authorize, in writing, subordinate officials under their jurisdiction to exercise the authority in their names. Such certification will identify, by position title, the following official in whose name the subordinate is acting:

(1) Headquarters Associate Administrators

(2) Center Directors

(3) Director, NASA Security Management Division

d. The NASA officials listed in 14 CFR Part 1203, Subpart H, Delegation of Authority to Make Determinations in Original Classification and Declassification Matters, are authorized to make, modify, or eliminate security classification assignments to information under their jurisdiction for which NASA has Original Classification Authority.

7. MEASUREMENT/VERIFICATION

a. Metrics will be focused on the NASA Strategic Plan to document performance and progress. Reports are to reflect the CY and are due quarterly on the 15th of the month following the end of each quarter and will cover the 3-month period immediately preceding the reporting date.

b. Incidents: Number of crimes against persons (e.g., murder, assault, rapes, robbery) occurring in the workplace; number and method of threats received.

c. Stolen Property: Dollar value of stolen property (e.g., Government, personal); number of items stolen; dollar value of items recovered.

d. Damaged or Destroyed Property: Dollar value of damaged property.

e. Security Clearances: Number of permanent clearances granted; number of clearances denied; number of clearances suspended; number of clearances revoked; number of clearances administratively reduced or increased, based upon direct support requirements to the NASA Strategic Plan.

f. Security Violations: Number of compromises of classified information; number of physical security compromises and other security program violations reported.

g. NASA Strategic Plan Support: Promote Center self-assessments as an Agencywide metric, i.e., reducing costs and paper work; eliminate unnecessary work or processes to facilitate personnel security, badging, classification management, physical security, communications security, information technology security programs, security education and briefings, and Agency actions related to implementation of Executive Orders and legislation impacting Agency security programs.

8. CANCELLATION

NPD 1600.2D, NASA Security Policy dated April 28, 2004.

Revalidated April 2, 2015, Original signed by

/s/ Sean O'Keefe

Administrator

ATTACHMENT A: (TEXT)

None.

(URL for Graphic)

None.

DISTRIBUTION: NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
