NASA Policy Directive

NPD 1600.2F
Effective Date: February 22, 2024
Expiration Date: February 22, 2029

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Subject: NASA Security Policy

Responsible Office: Office of Protective Services

1. POLICY

It is NASA's policy to provide protective services, as identified in this policy and described in NASA Procedural Requirements (NPR) 1600.1, NASA Security Program Procedural Requirements, which include law enforcement, security operations, 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 Federal laws, regulations, Executive Orders, other 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 is applicable to the Jet Propulsion Laboratory, a Federally Funded Research and Development Center, only to the extent specified in the NASA/Caltech Prime Contract.

b. This directive is applicable to other contractors, recipients of grants or cooperative agreements, or parties to other agreements only to the extent specified in contracts, grants or cooperative agreements, or other agreements.

c. Nothing in this directive is considered to limit the authorities of the Office of the Inspector General under the Inspector General Act of 1978, as amended.

d. 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 material.

e. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

3. AUTHORITY

The National Aeronautics and Space Act, 51 United States Code (U.S.C.) §§ 20132, 20133, 201344.

4. Applicable Document and Forms

NPR 1600.1, NASA Security Procedural Requirements.

5. RESPONSIBILITY

a. The Office of Protective Services (OPS) is responsible for organizing, establishing, and maintaining, in accordance with Federal laws, regulations, Executive orders, national level directives, and Agency requirements, a robust and comprehensive protective services program at NASA which includes law enforcement and security operations.

b. AA for OPS is NASA's Senior Agency Security Official, responsible for the functional management and leadership for the overall development, implementation, and maintenance of NASA Protective Services, including:

(1) Developing and issuing, subject to coordination with and approval by the NASA General Counsel, protective services policy, procedures, and guidelines, in collaboration with Center leadership, as appropriate.

(2) Establishing and maintaining an appropriate, consistent, and uniform law enforcement and security operation, 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 Code of Federal Regulations (CFR) pt. 1203b and 14 CFR pt. 1204, Subpart 10.

(3) Authorizing, under 51 U.S.C. Section 20133 and 20134, NASA Federal employees to carry firearms and exercise FAA in the course of their duties, and contractor and subcontractor employees to carry firearms and exercise Federal arrest authority 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.

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

(5) Serving as the Agency Risk Acceptance Authority (RAA) for all NASA security program risk management determinations that require a waiver of Agency security requirements. This does not include information technology (IT) Security RAA, which is the Chief Information Officer's (CIO) responsibility.

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

(7) Establishing and maintaining a Foreign National Access Management (FNAM) Program, led by OPS, in partnership with the Office of the Chief Information Officer (OCIO) and Office of International and Interagency Relations (OIIR).

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

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

(10) Establishing and maintaining a Personnel Security Program to manage eligibility for access to Classified National Security Information (CNSI), suitability for employment, and security screening for access to NASA Centers, Facilities, information, technology, and resources.

(11) Establishing and maintaining a CNSI program.

(12) Establishing and maintaining an Industrial Security Program to manage classified contracts.

(13) 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.

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

(15) Conducting periodic Program Reviews of Protective Service activities at Centers and Component Facilities to include protective services program self-assessments.

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

(17) Serving as the Senior Agency Official for the NASA Operational Security (OPSEC) Program as designated by the NASA Administrator and in accordance with National Security Presidential Memorandum (NSPM) -28, The National Operations Security Program.

(18) Developing, implementing, and maintaining policy formulation, oversight, coordination, and management of the Agency emergency management continuity of operations functions.

(19) Establishing and maintaining a Counterintelligence and Counterterrorism Program that is intended to protect the Agency against espionage, sabotage, other adversary intelligence activities, terrorism, or threats directed at NASA Federal and contract employees, facilities, operations, and information by deterring, detecting, and neutralizing potential threats posed by persons, organizations, or foreign powers.

(20) Developing, implementing, and maintaining appropriate and reasonable physical security controls at NASA

Centers and facilities.

(21) 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.

(22) Developing, implementing, and maintaining a Fire Services Program and Emergency Medical Services Program, including an integrated dispatch capability for protective services functions.

(23) Authorizing in writing other officials to exercise the responsibility(ies) and authority(ies) of the Senior Agency Security Official.

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

d. Center Directors are responsible for the following:

(1) Concurring with the appointment of a Center Chief of Protective Services (CCPS), after selection by the AA for OPS.

(2) Supporting local protective services procedures that ensure the successful implementation of this policy in accordance with NPR 1600.1.

(3) Maintaining awareness of threats directed against the Center, as well as the capabilities and limitations of the Center protective services program to counter such threats, in coordination with the AA/OPS, CCPS, and other OPS officials.

(4) Keeping the AA for OPS informed of any threats directed against the Center, including its operations, people, or property.

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

e. NASA Employees are responsible for complying with NASA Protective Services policies and procedural requirement and fully cooperate with protective services personnel during emergencies and during investigations or inquiries.

6. DELEGATION OF AUTHORITY

a. Authority is delegated by the Senior Agency Security Official to the Center Chief of Protective Services (CCPS) to suspend an employee's security clearance as outlined in Suspension and Removal, 5 U.S.C. § 7532.

b. Authority is delegated by the Senior Agency Security Official to the OPS Personnel Security Division to grant, deny, revoke, or suspend an Employee's security clearance in accordance with established procedural requirements.

c. Authority is delegated by the Senior Agency Security Official to the Center Chiefs of Protective Services to authorize NASA employees, and contractor and subcontractor employees to carry firearms and exercise Federal arrest authority 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.

d. Authority is delegated by the NASA Administrator to the officials designated below to make the determination and certification required by Security Requirements 51 U.S.C. § 20132 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) AA for OPS.

2) Deputy AA for OPS.

(3) Director, NASA Integrated Security Division, formerly NASA Security Management Division.

e. Authority is delegated by CNSI in accordance with E.O. 13526, to the officials designated below to make, modify, or eliminate security classification assignments to information under their jurisdiction for which NASA has Original Classification Authority:

(1) Deputy Administrator.

(2) Associate Administrator.

(3) AA for OPS.

(4) Deputy AA for OPS.

7. MEASUREMENTS

Perform Protective Services program reviews and Center Protective Services Office self-assessments to assess and reduce costs and paperwork; eliminate unnecessary work or processes; create and implement improved processes to facilitate protective services education and briefings; and Agency actions related to implementing Executive Orders and law.

8. CANCELLATION

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

/s/ Bill Nelson
Administrator

ATTACHMENT A: (TEXT)

Attachment A. References

A.1 Employment and Clearance; Individuals Removed for National Security, 5 U.S.C. 7312.

A.2 Security Requirements for Government Employees, E.O. 10450, 18 FR 2489 (1953).

A.3 National Industrial Security Program, E.O. 12829, 82 FR 3219 (2017).

A.4 Interagency Security Committee, E.O. 12977 (1995).

A.5 Reforming Process Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified Information, E.O. 13467, 73 FR 38103 (Jun. 30, 2008).

A.6 Classified National Security Information, E.O. 13526, 75 FR 1013 (Dec. 29, 2009).

A.7 Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, E.O. 13587, 76 FR 63811 (Oct. 7, 2011).

A.8 Suitability, 5 CFR pt. 731.

A.9 Delegation of Authority to Make Determinations in Original Classification Matters, 14 CFR pt. 1203 Subpt. H.

A.10 NASA Security Areas, 14 CFR pt. 1203a.

A.11 Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel, 14 CFR pt. 1203b.

A.12 Inspection of Persons and Personal Effects on NASA Installations or on NASA Property; Trespass or Unauthorized Introduction of Weapons or Dangerous Materials, 14 CFR pt. 1204 subpt. 10.

A.13 National Industrial Security Program Operating Manual and Supplement, 32 CFR pt. 117.

A.14 NPR 2841.1, Identity, Credential, and Access Management.

A.15 NASA-STD-8719.11, Standard for Fire Protection and Life Safety.

A.16 Federal Identity Credential and Access Management (FICAM) Roadmap.

A.17 Office of Management and Budget (OMB) Memorandum M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors (02/03/2011).

A.18 Security Executive Agent Directive (SEAD) 4, National Adjudicative Guidelines

A.19 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116.

A.20 NIST SP 800-79.

A.21 HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors.

A.22 Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

A.23 NSPM-28, The OPSEC Program.

Attachment B. Acronyms

CCPS Center Chief of Protective Services

CFR Code Federal Regulations

CIO Chief Information Officer

CNSI Classified National Security Information

DoD Department of Defense

E.O. Executive Order

FAA Federal Arrest Authority

FR Federal Register

FICAM Federal Identity, Credential, and Access Management

FIPS Federal Information Processing Standards

FNAM Foreign National Access Management

HSPD Homeland Security Presidential Directive

ICAM Identity, Credential, and Access Management

IT Information Technology

NIST National Institute of Standards and Technology

NISPOM National Industrial Security Program Operating Manual

NPR NASA Procedural Requirements

NRC Nuclear Regulatory Commission

NSPM National Security Presidential Memorandum

OCIO Office of the Chief Information Officer

OIIR Office of International and Interagency Relations

OMB Office of Management and Budget

OPS Office of Protective Services

OPSEC Official for the NASA Operational Security

PIV Personal Identity Verification

RAA Risk Acceptance Authority

SEAD Security Executive Agent Directive

SP Special Publication

U.S.C. United States Code

Attachment C. Protective Services Program Responsibilities

C.1 Establishing and maintaining a FNAM program that enables OPS to lead a partnership with OCIO and the OIIR in the coordination and organization of all NASA Foreign FNAM policies, procedures, and systems.

C.2 As a Federal law enforcement organization, establishing and maintaining appropriate law enforcement and security operations, including investigations, through the development, implementation, and management of FAA and Use of Force policies, procedures, processes, standards, and training as necessary to ensure strict compliance with 14 CFR pt 1203b-Security Programs; Arrest Authority and Use of Force by NASA Security Force Personnel and 14 CFR pt 1204, subpt 10, Inspection of Persons and Personal Effects on NASA Installations or NASA Property; Trespass or Unauthorized Introduction of Weapons or Dangerous Materials.

C.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.

C.4 Establishing and maintaining appropriate relationships with the national intelligence community to obtain and disseminate timely intelligence information, information on foreign intelligence collection efforts, and threat analysis.

C.5 Establishing and maintaining a Counterintelligence and Counterterrorism Program which is intended to protect the Agency against espionage, sabotage, other adversary intelligence activities, terrorism, or threats directed at NASA Federal and contract employees, facilities, operations, and information by deterring, detecting, and neutralizing potential threats posed by persons, organizations, or foreign powers.

C.6 Developing, implementing, and maintaining an Insider Threat Program, by E.O. 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, which is intended to deter, detect, and mitigate insider threat actions by all employees, both Federal, and contractor. In addition, 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.

C.7 Establishing, implementing, and maintaining an OPSEC Program, by NSPM-28, The National OPSEC Program, to identify and protect required critical assets, authorize required security assessments/inspections, identify and mitigate vulnerabilities, consider foreign adversarial threats in Agency organizational risk management activities, and apply sufficient threat mitigation practices to counter the threat.

C.8 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.

C.9 Ensuring that any person performing protective services 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.

C.10 Developing, implementing, and maintaining appropriate and reasonable physical security controls at NASA Centers and facilities by E.O. 12977, Interagency Security Committee, as amended by E.O. 13286, Presidential Policy Decision 21, Critical Infrastructure and Resilience and Department of Homeland Security, Interagency Security Committee Standards

C.11 Establishing NASA Security Areas by 14 CFR pt. 1203a.

C.12 Developing, implementing, and maintaining an Agency-wide Enterprise Identity, Credential, and Access Management (ICAM) program utilizing PIV Credentials, a PIV Card issuance program, and an integrated physical access control, video management, and intrusion detection system by the Federal Identity Credential and Access Management (FICAM) Roadmap, FIPS 201, OMB Memorandum M-11-11, and NIST Special Publication 800-116 and 800-79. 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.13 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.

C.14 Developing, implementing, and maintaining a robust Personnel Security Program for managing:

(a) Access to CNSI by Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to CNSI, E.O. 13467, CNSI and SEAD 4, National Adjudicative Guidelines.

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

(c) Appropriate security screening, by HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors, and Federal Information Processing Standards (FIPS) 201, 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 IT resources to ensure their continued reliability.

C.15 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 by the Department of Homeland Security National Terrorism Advisory System.

C.16 Establishing and maintaining a protective services education and awareness program designed to solicit the support and involvement of all its personnel.

C.17 Imposing administrative review of all business-related foreign travel by its employees when such review is appropriate in the interest of national security and the personal safety of the individual(s) involved.

C.18 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.

C.19 Applying Department of Defense (DoD) Industrial Security Program standards to NASA classified contracts by E.O. 12829, as amended by E.O. 12885, National Industrial Security Program, DoD 5220,22-M, the National Industrial Security Program Operating Manual (NISPOM) and the NISPOM Supplement.

C.20 Developing, implementing, and maintaining a CNSI program which is managed by E.O. 13526, and Information Security Oversight Office Directive Number 1, as amended.

C.21 Developing, implementing, and maintaining appropriate contingency plans for the effective and timely transition to emergency and threat environments.

C.22 Developing, implementing, and maintaining Fire Services by NASA Standard 8719.11 and Emergency Medical Services Programs by NPR 1800.1.

C.23 Developing, implementing, and maintaining an integrated Dispatch capability supporting Security, Law Enforcement, Safety and Health, and Fire and Rescue Services.

(URL for Graphic)

None.

DISTRIBUTION:
NODIS

This document does not bind the public, except as authorized by law or as incorporated into a contract. 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: https://nodis3.gsfc.nasa.gov.