NASA Policy Directive

NPD 2810.1F
Effective Date: January 21, 2022
Expiration Date: January 21, 2027

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Subject: NASA Information Security Policy

Responsible Office: Office of the Chief Information Officer

1. POLICY

a. This NASA Policy Directive (NPD) establishes information security policy for protecting both classified and unclassified information. Since NASA exists in a climate of persistent threats against its networks and systems, securing our information and technology is critical to achieve NASA's vision and to accomplish NASA's mission.

b. NASA's policy is to:

(1) Secure all NASA information and information systems, both classified and unclassified, in a manner that is commensurate with their national security classification level, sensitivity, value, and criticality.

(2) Fully implement the guidance in National Institute of Standards and Technology (NIST) Special Publication 800 series on computer security policies, procedures and guidelines, and the NIST Federal Information Processing Standards (FIPS) as directed in Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource" and the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq.

(3) Incorporate information security throughout the entire system life cycle to protect NASA information and information systems.

(4) Manage the cybersecurity of all classified and unclassified information systems that are acquired, developed, or used in support of NASA missions, programs, projects, and institutional partnerships through the complete system life cycle.

(5) Establish and manage sound risk management and cybersecurity processes.

(6) Conduct continuous monitoring and reviews of NASA information systems to verify compliance with applicable Federal laws and NASA policies.

(7) Investigate information security incidents and develop after action reports following significant incidents to address issues and improve future response.

(8) Ensure information security policy requirements, audits, and forensic investigations are implemented and coordinated across Centers and contracts.

(9) Implement applicable cybersecurity policy best practices and guidance.

(10) Ensure that software developed in support of NASA missions, programs, and projects, and used on NASA information systems, is secure.

(11) Ensure all information systems, classified and unclassified, operating within the NASA environment are operating under a valid authorization from an Authorizing Official per the Assessment and Authorization process.

2. APPLICABILITY

a. This NPD is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to the Jet Propulsion Laboratory (JPL), a Federally Funded

Research and Development Center, other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the contracts, grants, or agreements.

b. This NPD is applicable to all NASA users of information systems (e.g., civil servants and contractors) when supporting Agency projects, programs, and missions.

c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

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

3. AUTHORITY

a. Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

b. Inspector General Act of 1978, as amended, 5 U.S.C. App. III.

c. Cybersecurity Act of 2015, 6 U.S.C. § 1501 et seq.

d. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101 et seq.

e. Federal Information Security Modernization Act (FISMA) 2014, 44 U.S.C. § 3551 et seq.

f. Classified National Security Information, as amended, Executive Order (E.O.) 13526, 3 CFR 2009, Comp., p. 298.

g. Space Policy Directive-5: Cybersecurity Principles for Space Systems, 85 FR 56155-56158.

h. Circular A-130, Managing Information as a Strategic Resource, Office of Management and Budget, July 28, 2016.

4. APPLICABLE DOCUMENTS AND FORMS

a. Controlled Unclassified Information, E.O. 13556, 3 CFR 2009, Comp., p. 298.

b. Controlled Unclassified Information, 32 CFR pt. 2002.

c. NPD 1600.2, NASA Security Policy.

d. NPD 9800.1, NASA Office of Inspector General Programs.

e. NPR 2810.1, Security of Information Technology.

f. NPR 2841.1, Identity, Credential, and Access Management. e. Federal Information Processing Standards (FIPS), NIST.

g. Special Publication 800 Series, NIST.

5. RESPONSIBILITY

a. Responsibility for information security is primarily shared between the Office of the Chief Information Officer (OCIO), which is responsible for protecting unclassified information, and the Office of Protective Services (OPS), which is responsible for protecting classified information.

b. The NASA Administrator:

(1) Provides information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of NASA or within information systems used or operated by NASA, by a NASA contractor, or another organization on behalf of NASA.

(2) Ensures Agency information systems comply with the requirements of FISMA and other Federal laws, related policies, procedures, standards, and guidelines on unclassified information security and national security systems (i.e. classified systems).

(3) Ensures that information security management processes are integrated with NASA's strategic and operational planning processes.

(4) Ensures that senior NASA officials provide information security for the information and information systems that support the operations and assets under their control through:

(a) Assessing the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

(b) Determining levels of information security controls required to protect information and information systems and providing adequate information security resources to achieve them.

(c) Implementing policies and procedures for cost-effective risk management.

c. The NASA CIO:

(1) Ensures compliance with information security requirements.

(2) Develops and maintains an Agency-wide information security program by establishing and implementing cybersecurity policies and procedures, and by issuing and making broadly available instructions, memoranda, handbooks, and bulletins designed to facilitate protections.

(3) Ensures the development and maintenance of information security policies and procedures to protect unclassified information and ensure that sufficient resources are allocated to address information and information system security requirements.

(4) Oversees and ensures the training of key personnel with responsibilities for information security.

(5) Issues procedural requirements updates regarding protection and management of unclassified information and information systems to keep pace with the dynamic information security environment.

(6) Ensures procedures are established for referral, coordination, and assessment of suspected and confirmed incidents involving unclassified information systems and for referral to and coordination with the cognizant authorities.

(7) Charters suitable governance bodies as may be necessary to carry out this policy.

(8) Develops, implements, and maintains a Controlled Unclassified Information (CUI) program which is managed in accordance with E.O. 13556, 3 CFR, 2010, Comp., p. 267, Controlled Unclassified Information, and 32 CFR pt. 2002, Controlled Unclassified Information.

(9) Establishes a NASA information security capability for unclassified information and information systems with the mission and resources to:

(a) Develop and implement an information security review program designed to ensure that all NASA information systems used to process unclassified information are secure in compliance with NASA policy, NASA procedural requirements, and Federal guidelines and statutes (such as those listed in sections 3 and 4, and Attachment C), ensuring that reviews are coordinated with the NASA Office of Inspector General (OIG) to minimize duplicative review efforts.

(b) Investigate information security incidents involving sensitive information (e.g., Controlled Unclassified Information (CUI) [formerly referred to as Sensitive But Unclassified (SBU.)].)

(c) Support counterintelligence reviews, threat assessments, and investigations and issue NASA threat bulletins to protect unclassified information.

d. The NASA Assistant Administrator for OPS:

(1) In collaboration with NASA CIO, establishes a security program compliant with NPD 1600.2, NASA Security Policy.

(2) Ensures OPS responsibilities regarding Identity, Credential, and Access Management (ICAM) are addressed in accordance with NPR 2841.1, Identity, Credential, and Access Management.

(3) Develops and executes insider threat program processes and procedures that support information security objectives.

e. The officials in charge of Mission Directorates and Mission Support Offices:

(1) Participate with the NASA CIO and the Assistant Administrator for OPS in their respective development of NASA information security policies, standards, best practices, and guidance that protects NASA information and information systems.

(2) Ensure that adequate information security risk management design and planning is conducted to allow for effective cost-benefit analyses of alternate postures and of risk acceptance.

(3) Apply NASA policies and requirements, consistent with sound systems engineering and prudent risk management practices, for encryption and embedded software throughout the system life cycle and for other embedded IT, through design, development, test, and evaluation, until and through decommissioning.

f. The Senior Agency Information Security Officer (SAISO):

(1) Carries out the Agency CIO's responsibilities for information security.

(2) Establishes and manages the Agency Cybersecurity and Privacy Program and associated performance metrics.

(3) Maintains an office with the mission and resources for information security operations, cybersecurity governance, cybersecurity architecture and engineering, and cyber-threat analysis to assist in ensuring Agency compliance with Federal information security laws, directives, policies, standards, and guidelines.

(4) Manages the Agency's information security program and activities for unclassified information and information systems, including the preparation and maintenance of NPR 2810.1, Security of Information Technology.

(5) Monitors cybersecurity risk-related considerations and risk management of individual information systems to ensure they are consistent across the Agency, are viewed from an Agency-wide and strategic goal perspective and reflect the Agency's information system risk tolerance affecting mission/business success. Monitoring activities will align with roles and responsibilities of the Risk Executive promulgated by NIST.

g. The Center Directors and the Director for Headquarters Operations:

(1) Ensure compliance with this directive, NASA policies, procedures, requirements, and the Federal information security policy for activities under their purview.

(2) Apply these policies and requirements, consistent with sound systems engineering and prudent risk management practices, for encryption and embedded software throughout the system life cycle and for other embedded IT, through design, development, test, and evaluation, until and through decommissioning.

h. The Center CIOs and the Headquarters CIO are responsible and accountable for the protection of information and information systems under their purview as well as compliance with this directive, NASA information security policies, procedures, and Federal information security laws, directives, policies, and standards.

i. The Center Chief Information Security Officer (CISO):

(1) Oversees the implementation of information security policies for their Center.

(2) Assists the SAISO and the Center CIO, with adequate resources, implementing this directive by executing and enforcing the NASA Cybersecurity and Privacy Program; Federal information security laws, directives, standards; and applicable guidelines; and provides adequate resources to ensure their compliance at the Center level.

(3) Serves as the primary interface between the SAISO and Center information security functions.

(4) Is responsible for the coordination of investigations of unclassified information security incidents to include:

(a) Referring an information security incident to the appropriate investigating authority.

(b) Referring suspected computer crimes to the NASA OIG and cooperating and assisting the NASA OIG with its investigation of computer crimes, as requested.

(c) Referring information security incidents with a counterintelligence nexus to the NASA Counterintelligence Director.

(5) Monitors cybersecurity risk management implementation at their Center, in support of the SAISO's risk management responsibilities.

j. NASA Users adhere to all NASA information security policies, processes, and procedures.

6. DELEGATION OF AUTHORITY

This NPD authorizes the delegation of Agency CIO's responsibilities for information security to the SAISO in accordance with FISMA.

7. MEASUREMENTS

None.

8. CANCELLATION

NPD 2810.1E, NASA Information Security Policy, dated January 31, 2020.

/s/ Bill Nelson
Administrator

ATTACHMENT A. DEFINITIONS

Cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Information. Any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, produced for, or is under the control of NASA.

Information Security. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Incident. Any adverse event or situation associated with a system that poses a threat to the system's integrity, availability, or confidentiality. For example, an incident may result in or stem from any one of the following: a failure of security controls; an attempted or actual compromise of information; and/or waste, fraud, abuse, loss, or damage of government property or information.

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. This term incudes both Operational Technology and Information Technology.

Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data by the Agency. This includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. NASA Center. Any of the collection of facilities and installations designated by NASA, and usually grouped by function (e.g., research, construction, administration).

(NASA) Mission Directorate. Any of the four chartered offices and personnel overseeing Aeronautics Research, Human Exploration and Operations, Science, and Space Technology.

(NASA) Mission Support Office. The office and personnel chartered to support the various corporate needs of the NASA Mission Directorates, including Human Capital Management, Procurement, Protective Services, and the management of information technology under the OCIO.

NASA User. Any explicitly authorized patron of a NASA information system. National Security System. Any NASA information system designated as being authorized to process CNSI.

Operational Technology. Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

Program. A strategic investment by a Mission Directorate or Mission Support Office that has a defined architecture and/or technical approach, requirements, funding level, and a management structure that initiates and directs one or more projects. A program defines a strategic direction that the Agency has identified as needed to accomplish Agency goals and objectives.

Project. A specific investment identified in a Program Plan having defined requirements, a life-cycle cost, a beginning, and an end. A project also has a management structure and may have interfaces to other projects,

agencies, and international partners. A project yields new or revised products that directly address NASA?s strategic needs.

Risk. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Senior Agency Information Security Officer. The official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

Unclassified Information. All information that does not meet the criteria described in E.O. 13526, 3 CFR, 2009 Comp., p. 298. Federal requirements for protecting unclassified information are prescribed in FISMA.

ATTACHMENT B. ACRONYMS

CFR - Code of Federal Regulations

CIO - Chief Information Officer

CISO - [Center] Chief Information Security Officer

e.g. - exempli gratia (for example)

e-Gov - Electronic Government

EO - Executive Order

FIPS - Federal Information Processing Standards

FISMA - Federal Information Security Modernization Act

FR - Federal Register

ICAM - Identity, Credential, and Access Management

IT - Information Technology

JPL - Jet Propulsion Laboratory

NASA - National Aeronautics and Space Administration

NIST - National Institute of Standards and Technology

NODIS - NASA Online Document Information System

NPD - NASA Policy Directive

NPR - NASA Procedural Requirement

OCIO - Office of the Chief Information Officer

OIG - Office of Inspector General

OMB - Office of Management and Budget

OPS - Office of Protective Services

SAISO - Senior Agency Information Security Officer

SBU - Sensitive But Unclassified

SP - Special Publication

URL - Uniform Resource Locator

U.S.C. - United States Code

ATTACHMENT C. REFERENCES

C.1. The following authority documents provide additional statutory requirements for information security:

a. Paperwork Reduction Act of 1995, 44 U.S.C. § 3501, et seq., as amended.

b. E-Government (e-Gov) Act of 2002, as amended, 44 U.S.C. § 3601 et seq.

c. National Aeronautics and Space Act, 51 U.S.C. § 20101 et seq.

d. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, EO 13800, May 11, 2017, 82 FR 22391.f.

C.2. The following reference documents will aid in the understanding of this NPD:

a. NPR 1600.1, NASA Security Program Procedural Requirements.

b. NPR 1600.3, Personnel Security.

c. OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act, December 23, 2016.

d. OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, July 15, 2016.

e. OMB Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Actions and Milestones, October 17, 2001.

f. OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

g. OMB M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006.

h. OMB M-06-16, Protection of Sensitive Agency Information, June 23, 2006.

i. NIST Cybersecurity Framework, (URL: https://www.nist.gov/cyberframework/framework).

j. NIST 800-59, Guideline for Identification of Information Systems as National Security Systems, August 2003. k. https://www.cisa.gov/securing-federal-networks

(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.