

[| NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

# NASA Policy Directive

**NPD 2800.1F**Effective Date: January 11, 2025  
Expiration Date: January 11, 2030**COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES**[Printable Format \(PDF\)](#)

---

## Subject: Managing Information Technology (Updated with Change 1)

**Responsible Office: Office of the Chief Information Officer**

### Change Log

Chg#	Date	Description/Comments
1	04/02/2025	Administrative edit made in section 3 to comply with an executive action. The reference to EO 14110, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023, was removed because it was rescinded by EO 14179, Removing Barriers to American Leadership in Artificial Intelligence, dated January 23, 2025.

### 1. POLICY

- a. It is NASA policy to ensure that information technology (IT) and information resources are planned, acquired, and managed in a manner that complies with the policies, procedures, and priorities of the Agency and the Federal Government.
- b. It is NASA policy to govern NASA's IT direction, mission alignment, investments, and accountability to maximize the value of the Agency's IT contribution to NASA's missions, partners, and the public.
- c. It is NASA policy to strategically manage and operate IT and information resources to support achievement of the Agency's goals and objectives. IT management and operations promote the effective, secure, and efficient use of IT and data throughout the Agency to increase productivity and safety while enabling robust operation, responsiveness, and effectiveness of the Agency's programs.
- d. It is NASA policy to curate, govern, and strategically manage data in alignment with the Agency's missions and Federal regulations, ensuring data-driven insights to advance Agency goals, while promoting data integrity, security, accessibility, and utility for stakeholders, partners, and the public.

### 2. APPLICABILITY

- a. This directive is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers (Agency-wide).
- b. 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 expected outcome, and "are/is" denotes descriptive material.
- c. This NASA Policy Directive (NPD) applies to all NASA IT and information resources as defined by United States

Federal Code 40 U.S.C. 11101, including operational technology and mission systems. This definition of IT applies unless expressly excluded by the NASA Chief Information Officer (CIO).

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

### **3. AUTHORITY**

- a. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 et seq.
- b. Agency Chief Information Officer, 40 U.S.C. §11315.
- c. The Federal Information Technology Acquisition Reform Act (FITARA), 2014, 40 U.S.C. §11319.
- d. Federal Agency Responsibilities, 44 U.S.C. §3554.
- e. E-Government Act of 2002 (Public Law 107-347), as amended, 44 U.S.C. 3601 et seq.
- f. Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. 113-283 (2014).
- g. Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. 115-435 (2019).
- h. Improving the Nation's Cybersecurity, E.O. 14028 (2021).
- i. NPD 1000.3, The NASA Organization.
- j. NPD 1210.7, NASA Evaluation Policy.

### **4. APPLICABLE DOCUMENTS AND FORMS**

- a. NASA FAR Supplement, Enterprise Procurement Strategies, Appendix A, 48 CFR § A-102.2.
- b. NPD 1001.0, NASA Strategic Plan.
- c. NPR 2810.1, Security of Information and Information Systems.
- d. NASA Information Technology Strategic Plan.
- e. NASA Data Strategy.

### **5. RESPONSIBILITY**

- a. The NASA CIO:

- (1) Advises and assists the Administrator and other Agency senior staff on IT management and operations.
- (2) Advises the Administrator whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component.
- (3) Coordinates with the Administrator and Chief Financial Officer (CFO) to manage the IT for business operations. Management activities include conducting feasibility studies for financial systems, approving and managing financial management systems design and enhancement projects, developing requirements, implementing systems, and auditing the financial information for reliability and the operations for performance evaluation.
- (4) In partnership with the CFO, defines the level of detail at which IT resource levels are described distinctly from other resources throughout the planning, programming, and budgeting stages. Uses this detail as the primary input into the IT capital planning and investment control.
- (5) Coordinates with Mission Directorates, the Mission Support Directorate, and Mission Support Enterprise Organizations on IT matters and represents the Agency in Federal activities involving IT or information management.
- (6) Ensures the successful completion of related E-Government actions.
- (7) Leads strategic management activities. Develops and publishes the NASA IT Strategic Plan. Establishes, articulates, and adjusts NASA's IT vision, strategy, outcomes, priorities, and metrics in coordination with Mission Directorates, the Mission Support Directorate, Mission Support Enterprise Organizations, and Centers. Monitors and assesses IT-related performance to enable achievement of the goals and outcomes set forth in NPD 1001.0, NASA

Strategic Plan, and the NASA IT Strategic Plan. Ensures that IT investments align with the goals and outcomes in the NASA Strategic Plan and the NASA IT Strategic Plan and allocates resources in support of IT goals and outcomes.

(8) Leads NASA's IT budget formulation, portfolio management, and investment oversight. Manages IT investment resources by ensuring that IT and information resources are strategically managed to achieve NASA's goals and objectives. Maintains responsibility and accountability for Agency IT investments. Has a significant role in IT execution decisions and the management, governance, and oversight processes related to IT including portfolio review, evaluating IT investments according to the risk (i.e., IT Dashboard CIO ratings on [www.itdashboard.gov](http://www.itdashboard.gov)) and reviewing high-risk IT investments. Selects, controls, and evaluates IT investments by defining and implementing Capital Planning and Investment Control, Enterprise Architecture (EA), program and project management, and reporting policies to align with NASA's Planning, Programming, Budgeting, and Execution process. Analyzes and optimizes the Agency's IT investment portfolio across NASA's IT programs, Centers, and Mission Directorates. Approves NASA's IT budget request. Develops IT operating and execution plans, executes the budget during the performance cycle, and oversees the budget across the IT portfolio. Certifies that IT resources are adequately implementing incremental development, as defined in capital planning guidance issued by the Office of Management and Budget (OMB).

(9) Leads IT program and project management activities. Establishes and supports a structured approach to manage IT Service Lines (SLs) and Agency Level Offices (ALOs). Conducts IT policy and compliance management, including developing, implementing, and enforcing Agency policies, procedures, control techniques, standards, guidelines and overall policies for reporting related to IT and information resources. Aligns resources and oversees implementation of supporting IT policies, SLs, and efforts. Manages IT SLs as integrated collections of end-to-end services that increase cybersecurity, efficiency, and inter-Center collaboration. Conducts reviews of SL and project performance, evaluates the current and projected status toward established requirements, objectives, and performance goals. Establishes and maintains a process to regularly engage with SL leaders to evaluate IT resources supporting each NASA strategic objective.

(10) Communicates and reports information concerning NASA's IT activities. Maintains an inventory of data centers and a strategy to consolidate and optimize data centers. Performs IT reporting, including by overseeing IT reporting as required by Congress, OMB, the Government Accountability Office, and other external entities. Prepares an annual report on the progress in achieving NASA's IT strategic outcomes.

(11) Manages IT information security and risk. Develops and maintains information security policies, procedures, and control techniques. Ensures that senior Agency officials, including Center CIOs, carry out their information security responsibilities as detailed in NASA Procedural Requirement (NPR) 2810.1, Security of Information and Information Systems. Integrates risk management into the Agency's IT processes to identify, assess, prioritize, and manage risks. Safeguards NASA's data and IT assets through an Agency-wide cybersecurity mitigation planning and risk reduction.

(12) Conducts IT governing activities. Under the NASA CIO's delegated authority in NPD 1000.3 Chapter 4, charters boards to facilitate IT governing activities to evaluate the Agency's business conditions and needs, set strategy and direction, and oversee performance outcomes. Establishes, maintains, and communicates the Agency-wide IT governing structure. Participates on all governance boards that include IT resources as specified in the board Charters.

(13) Establishes Agency EA that aligns with and supports the Agency's Strategic Plan, capital planning process, and service delivery strategy. Designates NASA Chief Enterprise Architect (CEA) to manage and maintain the Agency's EA.

(14) Conducts IT workforce planning. Ensures the competency and motivation of NASA's IT workforce through effective recruiting, hiring, training, mentoring, professional development, and incentives to support achievement of NASA's missions, goals, and objectives. Develops annual strategies for hiring and training to rectify any knowledge and skill deficiencies. Reports annually to the NASA Administrator on progress made in improving IT personnel capabilities.

(15) Develops IT innovation by identifying, testing, and implementing emerging IT and processes in support of NASA's changing technology and business needs. Engages stakeholders in data management, data standards, interoperability, open innovation, artificial intelligence, and technology infusion in alignment with Agency priorities. Develops roadmaps to reinforce the linkage between IT innovation and OCIO strategy.

(16) Performs IT contract management for NASA IT investments and contracts that include IT by managing the lifecycle of current and planned IT contracts, including delivery of IT products and services by third party vendors and external service providers. Oversees contract performance. Reviews and approves IT contracts, acquisition plans, or strategies. Ensures that IT supply and service purchases comply with mandatory IT enterprise contracts listed under

NASA Federal Acquisition Regulation (FAR) Supplement, Enterprise Procurement Strategies, 48 CFR §A-102.2.

(17) Performs continuous improvement. Benchmarks Agency processes against the private and public sectors to promote continuous improvement of IT services and management. Ensures that NASA processes are analyzed and optimized before making significant investments.

b. The members of the CIO Senior Advisory Team (SAT) operate as extensions of the NASA CIO and help shape the strategic direction and operational evolution of IT services and data. The Deputy Chief Information Officers (DCIOs) share accountability with the NASA CIO for oversight and management of IT assets and services, and selecting and managing SL Directors, ALO Chiefs, and Center CIOs. DCIOs also provide oversight of the planning, design, integration, and delivery of NASA's IT projects and services and exercise IT authority, including investment review, architecture compliance, and cybersecurity compliance for all IT. The SAT conducts cybersecurity risk mitigation planning, compliance, risk reduction and accelerates and coordinates digital advances to transform the way the Agency works.

c. The Senior Agency Information Security Officer (SAISO) carries out the CIO's responsibilities for development, documentation, and implementation of the Agency-wide information security and privacy program.

d. The NASA Chief Data Officer (CDO) develops, documents, and implements NASA data policies, data governance, and data lifecycle. The CDO serves as the OCIO designated official for the use, protection, dissemination, and generation of data. In that capacity, the CDO works closely with the NASA Chief Artificial Intelligence (CAIO) Officer, leads and coordinates OCIO support to the CAIO and serves on the agency artificial intelligence governance.

e. The NASA Digital Transformation Office Chief synchronizes and catalyzes NASA's digital transformation strategies, plans, and investments across the OCIO, Mission Directorates, the Mission Support Directorate, and Mission Support Enterprise Organizations to minimize duplication and maximize mission impact.

f. The NASA CEA establishes and maintains EA governance structures, policies, and procedures to guide EA development, integration, and evolution across the Agency. The CEA oversees the development and maintenance of comprehensive EA artifacts that align with the Agency's Strategic Plan, capital planning process and service deliver strategy. The artifacts include business, data, application, cyber security, and technology architectures that provide a holistic view of the Agency's IT landscape.

g. The Agency Software Manager (ASM) leads NASA efforts to centralize software license management, implement strategies to reduce duplication, and ensure the adoption of software management best practices.

h. Center Directors:

(1) Ensure compliance with IT policies and procedures.

(2) Ensure proper integration of IT programmatic and operational needs of the program and projects assigned to their Center.

(3) Provide stakeholder input to the OCIO toward the formulation of future IT program and project strategy.

(4) Communicate any issues to the OCIO and participates in strategy discussions as appropriate.

i. Center CIOs:

(1) Operate as an extension of the NASA CIO and help shape strategic direction and evolution of IT services.

(2) Act as a representative on IT matters at their Centers by managing business management, customer engagement, and service integration activities and act as a liaison between Center customers and the Agency OCIO organization.

(3) Provide local business management, customer engagement, and integration for SL provided services and local customers.

(4) Collaborate with the ALOs to provide integration for services and solutions for Center, mission, and mission support requirements.

(5) Perform Center Delivered Services as defined in coordination with Center Director and OCIO.

(6) Participate and comply with IT policy and governance processes.

j. Mission Directorate Associate Administrators identify an Agency-level representative for Mission IT matters to coordinate with OCIO by:

- (1) Developing IT policies and procedures for mission systems in partnership with OCIO per the flow and order of precedence in NPD 1400.1, Documentation and Promulgation of Internal NASA Requirements, Attachment C.
- (2) Monitoring, managing, mitigating, and accepting identified mission-related cybersecurity risks in accordance with Agency policy, including but not limited to NPR 2810.1.
- (3) Ensuring mission programs and organizations participate and comply with IT policy and governance processes.
- (4) Participating in IT governance boards.

## 6. DELEGATION OF AUTHORITY

The NASA CIO exercises two types of authorities:

- (1) IT Authority, which refers to portfolio investment insight and oversight, EA compliance, policy compliance, and cybersecurity compliance for all NASA IT, information resources, data, and information. IT Authority provides insight and influence on all IT investments in order to mitigate resource risks by using data to drive better purchasing of hardware, software, and services and to enable proper cybersecurity mitigation planning and risk reduction. The NASA CIO may delegate IT Authority to Deputy CIOs, the SAISO, the CDO, the Agency's Digital Transformation Officer (DTO), Center CIOs, ASM, the Enterprise Business Management Office Chief, the Program Manager for Agency Business Solutions, SL Directors, ALO Chiefs, and Center CIOs.
- (2) IT Program Authority, which refers to the management oversight, implementation, and operations of IT services and products. The NASA CIO exercises IT Program Authority for services managed by the NASA CIO as defined in the IT Service Portfolio. The NASA CIO may delegate IT Program Authority to Deputy CIOs, Center CIOs, SAISO, CDO, DTO, the Enterprise Business Management Office Chief, ASM, the Program Manager for Agency Business Solutions, SL Directors, ALO Chiefs, or Center CIOs.

The NASA CIO delegates to DCIOs, Center CIOs, CDO, CAIO, SAISO, DTO, ASM, Program Managers, SL Directors, and ALO Chiefs IT Authority and IT Program Authority the accountability and responsibility to ensure that NASA IT strategies, policies, architectures, investments, support services, procedures, standards, guidelines, and practices align with Federal and Agency requirements and directions. The NASA CIO has the authority to delegate the role of Authorizing Official for select NASA mission systems, Programs, and Projects.

## 7. MEASUREMENTS/VERIFICATION

Outcomes and performance measures related to the implementation of this policy are outlined in documents such as NPD 1001.0, the NASA Data Strategy, and the NASA IT Strategic Plan, as well as in IT and data-related metrics in NASA's Annual Performance Plan and Federal cross-agency initiatives. Verification occurs through the NASA CIO's performance monitoring and the Agency's Baseline Performance Review. Results are reported through NASA's annual strategic review, NASA's annual Volume of Integrated Performance, the Agency's annual statement of assurance process, reporting for Federal Information Security Modernization Act of 2014, Pub. L. 113-283 (2014), reporting requirements of Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. 115-435 (2019) and reporting as directed by OMB.

## 8. CANCELLATION

NPD 2800.1E, Managing Information Technology, December 9, 2019.

---

**/s/ Administrator**  
**Administrator**

---

### Attachment A. Definitions

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



**Attachment B. Acronyms**

AI - Artificial Intelligence  
ALO - Agency Level Office  
ASM - Agency Software Manager  
CAIO - Chief Artificial Intelligence Officer  
CCIO - Center Chief Information Officer  
CDO - Chief Data Officer  
CEA - Chief Enterprise Architect  
CFO - Chief Financial Officer  
CIO - Chief Information Officer  
DCIO - Deputy Chief Information Officer  
DTO - Digital Transformation Officer  
EA - Enterprise Architecture  
FISMA - Federal Information Security Modernization Act  
IT - Information Technology  
NASA - National Aeronautics and Space Administration  
NPD - NASA Policy Directive  
NPR - NASA Procedural Requirements  
OCIO - Office of the Chief Information Officer  
OMB - Office of Management and Budget  
SAISO - Senior Agency Information Security Officer  
SAT - Senior Advisory Team  
SL - Service Line  
U.S.C. - United States Code

**ATTACHMENT C: References**

C.1 The Rehabilitation Act, 29 U.S.C. 794d, Sec. 508.  
C.2 Preparation, Submission, and Execution of the Budget, OMB Circular A-11.  
C.3 Management of Federal Information Resources, OMB Circular A-130.  
C.4 NPD 1440.6, NASA Records Management.  
C.5 NPD 1490.1, NASA Printing, Duplicating, and Copying Management.  
C.6 NPD 2200.1, Management of NASA Scientific and Technical Information.  
C.7 NPD 2800.1, Managing Information Technology.  
C.8 NPD 2810.1, NASA Information Security Policy.  
C.9 NPD 2830.1, NASA Enterprise Architecture.  
C.10 NPR 1382.1, NASA Privacy Procedural Requirements.  
C.11 NPR 7120.7, NASA Information Technology Program and Project Management Requirements.

C.12 IT Service Portfolio OCIO Product and Service Portfolio - All Documents (nasa.gov) (Internal to NASA only).

**(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>.**

---