NASA Policy Directive

NPD 2800.1E
Effective Date: December 09, 2019
Expiration Date: December 09, 2024

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Printable Format (PDF)

Subject: Managing Information Technology, Updated w/Change 3

Responsible Office: Office of the Chief Information Officer

CHANGE HISTORY

Chg#	Date	Description/Comments
1	12/17/2021	Update to comply with 1400 Compliance,with administrative changes, update applicable documents, and added Attachment -References.
2	02/01/2022	Updated with administrative changes made to comply with 1400, update applicable documents, and added Attachment -References.
3	10/11/2023	Updated with administrative changes made to add a policy statement in Section 1, authorities in Section 3, an applicable document in Section 4, and the role of the NASA Chief Data Officer in Section 5 all of which the Agency is currently operating under. Section 7 was also clarified and Attachments B and C were updated.

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 IT activities by ensuring that IT and information resources support achievement of the Agency's goals and objectives. Strategic IT management activities promote the effective, secure, and efficient use of IT 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 terms "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, including operational technology, as defined by U.S. Federal Code 40 U.S.C. 11101, and mission systems. IT and information resources are defined as any equipment or system that is used in the acquisition, storage, retrieval, manipulation and/or transmission of data or information. Information resources include computers, ancillary and peripheral equipment, software, firmware, and physical devices. This definition 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.

e. The NASA CIO exercises two types of authorities:

(1) IT Authority, which refers to portfolio investment insight and oversight, enterprise architecture compliance, policy compliance, and cybersecurity compliance for all NASA IT and information resources. 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 and software and to enable proper cybersecurity mitigation planning and risk reduction. The NASA CIO may delegate IT Authority to Associate CIOs (ACIOs) and IT Program Executives (PEs).

(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. The NASA CIO may delegate IT Program Authority to an Associate CIO or Center CIO.

3. AUTHORITY

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

b. The Federal Information Technology Acquisition Reform Act (FITARA), 2014, 40 U.S.C. § 11319.

c. E-Government Act of 2002 (Public Law 107-347), as amended, 44 U.S.C. 3601 et seq.

d. Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. 113-283 (2014).

f. Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. 115-435 (2019).

g. NPD 1000.3, The NASA Organization.

h. 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 Plan.

5. RESPONSIBILITY

a. The NASA CIO:

(1) Advises and assists the Administrator and other Agency senior staff, and participates on the Agency Strategic Management Council, Mission Support Council, and Agency Program Management Council.

(2) Advises the Administrator whether to continue, modify, or terminate any acquisition, investment, or activity that includes a significant IT component. Coordinates with the Administrator and CFO to ensure that the Financial systems are established and implemented per the requirements of Clinger-Cohen Act of 1996, 40 U.S.C § 11101 et seq. In partnership with the Chief Financial Officer (CFO), defines the level of detail at which IT resource levels are described.

(3) Coordinates with Mission Directorates and the Mission Support Directorate on IT matters and represents the Agency in Federal activities involving IT or information management and ensuring the successful completion of

related E-Government actions.

(4) 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 risk (i.e., IT Dashboard CIO ratings) and reviewing high-risk IT investments. Selects, controls, and evaluates IT investments using the Capital Planning and Investment Control (CPIC) process in alignment with NASA's Planning, Programming, Budgeting, and Execution (PPBE) 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 OMB.

(5) Leads IT program and project management activities. Establishes and supports a structured approach to manage IT programs. Conducts IT policy and compliance management, including developing, implementing, and enforcing Agency policies, procedures, control techniques, standards, guidelines and overall polices for reporting related to IT and information resources. Aligns resources and oversees implementation of supporting IT policies, programs, and activities. Manages IT programs as integrated end-to-end services that increase cybersecurity, efficiency, and inter-Center collaboration. Conducts reviews of program 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 program managers to evaluate IT resources supporting each NASA strategic objective.

(6) Leads strategic management activities. Establishes, articulates, and adjusts NASA's IT vision, strategy, outcomes, priorities, and metrics in coordination with Mission Directorates, the Mission Support Directorate, and Centers. Monitors and assesses IT-related performance to enable achievement of the goals and outcomes in the NPD 1001.0 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.

(7) 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, the Office of Management and Budget (OMB), the Government Accountability Office (GAO), and other external entities. Prepares an annual report on the progress in achieving NASA's IT strategic planning goals.

(8) Manages IT information security and risk. Ensures that senior Agency officials, including Center CIOs, carry out their information security responsibilities as detailed in 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.

(9) Designates, selects, and manages a member of the CEC to represent Agency IT matters, Center CIOs, the Senior Agency Information Security Officer (SAISO), a Senior Agency Official for Privacy (SAOP) and the Agency Chief Data Office (CDO).

(10) Conducts IT governing activities. Under the NASA CIO's delegated authority from the Information Technology Council (ITC), 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, including any Agency-, Mission Directorate-, Mission Support Directorate-, or Center-level investment review boards.

(11) Oversees NASA's enterprise architecture (EA) by developing, implementing, and maintaining NASA's IT EA in alignment with Federal and NASA policies and guidance.

(12) 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.

(13) 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, and technology infusion in alignment with Agency priorities.

(14) Performs IT contract management for NASA IT investments and contracts that include IT by managing the life

cycle 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 FAR Supplement, Enterprise Procurement Strategies, 48 CFR § A-102.2.

(15) 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. Associate CIOs operate as an extension of the NASA CIO and shape the strategic direction and evolution of IT services. Share accountability with the NASA CIO for effective oversight and management of IT assets and services. Select and manage IT Program Executives, with the concurrence of the NASA CIO. Provide oversight of the planning, design, integration, and delivery of NASA's IT projects and services. Exercise IT authority, including investment review, architecture compliance, and cybersecurity compliance for all IT to mitigate resource risks. Conduct cybersecurity risk mitigation planning, compliance, and risk reduction.

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

d. The NASA Chief Data Officer (CDO) ensures Agency compliance with the law, including development, documentation, and implementation of NASA data policies, data governance, and data lifecycle management.

e. The Center Director and Mission Directorate Associate Administrator:

(1) Communicate with Center CIOs and Mission Directorate IT Representatives to identify gaps in IT services and elevate critical issues.

(2) Provide visibility into Center and Mission Directorate IT investments to enable mitigation of Agency-wide IT resource and cybersecurity risks.

(3) Implement risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. Ensure that cybersecurity risk management processes are aligned with strategic, operational, and budgetary planning processes.

(4) Ensure that their programs and projects implement cybersecurity requirements established in NPR 2810.1, Security of Information Technology.

f. Center CIOs:

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

(2) Share accountability with the NASA CIO for effective implementation, operations, utilization, and evaluation of IT services.

(3) Exercise delegated IT authority for all IT within the Center, in partnership with the IT Program Executives.

(4) Act as a representative on IT matters at their Centers.

(5) Implement a Center IT governance process that is supportive of, aligned with, and integrates with the Agency IT governance process. Participate in other Center governance processes where IT is included. Collaborate with stakeholders to identify requirements to improve IT services. Provide the NASA CIO with visibility into and awareness of Center IT.

g. Mission Directorates:

(1) Identify an Agency-level IT Representative to ensure mission entities and IT matters are represented in the development of policies and procedures, especially those pertaining to cybersecurity.

(2) Enable mitigation of Agency-wide IT resource and cybersecurity risks.

(3) Ensure mission programs and organizations participate and comply with IT policy and governance processes. Participate in governance boards.

6. DELEGATION OF AUTHORITY

The NASA CIO delegates to Associate CIOs, Center CIOs, and IT Program Executives IT Authority and IT Program Authority, as well as 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. Center CIOs, Associate CIOs, and IT Program Executives shall support the NASA CIO in the discovery and analysis of IT investments and ensure compliance of IT investments with the Agency's policies and procedures. Delegate the role of Authorizing Official for select NASA mission systems Programs and Projects.

7. MEASUREMENT/VERIFICATION

Outcomes and performance measures related to the implementation of this policy are outlined in documents such as NPD 1001.0, 2022 NASA Strategic Plan, 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 (BPR). Results are reported through NASA's annual strategic review, NASA's annual Volume of Integrated Performance, the Agency's annual statement of assurance process, FISMA reporting, OPEN Data Act Reporting and reporting as directed by OMB.

8. CANCELLATION

NPD 2800.1A, Managing Information Technology, March 21, 2008.

REVALIDATED ON 1/10/22, ORIGINAL SIGNED BY /s/Jim Bridenstein Administrator

ATTACHMENT A: Definitions

Operational Technology (OT) - Hardware and software that is physically part of, dedicated to, or essential in real time to the performance, monitoring, or control of physical devices and processes.

ATTACHMENT B: Acronyms

ACIO - Associate Chief Information Officer

BPR - Baseline Performance Review

CDO - Chief Data Officer

CEC - CIO Executive Council

CFO - Chief Financial Officer

CIO - Chief Information Officer

CPIC - Capital Planning and Investment Control

EA - Enterprise Architecture

FISMA - Federal Information Security Modernization Act

FITARA - Federal Information Technology Acquisition Reform Act

GAO - Government Accountability Office

IT - Information Technology

ITC - Information Technology Council

NASA - National Aeronautics and Space Administration

NPD - NASA Policy Directive

NPR - NASA Procedural Requirements

OMB - Office of Management and Budget

PE - Program Executive

PPBE - Planning, Programming, Budgeting and Execution

US - United States

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 1000.0, NASA Governance and Strategic Management Handbook.

C.5 NPD 1000.3, The NASA Organization.

C.6 NPD 1440.6, NASA Records Management.

C.7 NPD 1490.1, NASA Printing, Duplicating, and Copying Management.

C.8 NPD 2081.1, Nondiscrimination in Federally Assisted and Conducted Programs of NASA.

C.9 NPD 2200.1, Management of NASA Scientific and Technical Information (STI).

C.10 NPD 2810.1, NASA Information Security Policy.

C.11 NPD 2830.1, NASA Enterprise Architecture.

C.12 NPD 7120.4, NASA Engineering and Program/Project Management Policy.

C.13 NPR 1382.1, NASA Privacy Procedural Requirement.

C.14 NPR 2800.1, Managing Information Technology.

C.15 NPR 2810.1, Security of Information Technology.

C.16 NPR 2830.1, NASA Enterprise Architecture Procedures.

C.17 NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

C.18 NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements.

C.19 NPR 7150.2, NASA Software Engineering Requirements.

C.20 NASA IT Strategic Plan.

C.21 NASA Data Strategy Plan

C.22 OMB M-19-23, Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance

(URL for Graphic)

None.

DISTRIBUTION:
NODIS