U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (MD)

MD 2.6	INFORMATION TECHNOLOGY INFRASTRUCTURE AND END USER SERVICES	DT-21-13
Volume 2	Information Technology	
Approved By:	Daniel H. Dorman Executive Director for Operations	
Date Approved:	December 9, 2021	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of the Chief Information Officer IT Services Development and Operations Division	
Contact Name:	Rachel Johnson	

EXECUTIVE SUMMARY

Management Directive (MD) 2.6, "Information Technology Infrastructure," has been expanded and renamed, "Information Technology Infrastructure and End User Services."

This MD includes, and updates previous guidance found in MD 2.3, "Telecommunications," and MD 2.7, "Personal Use of Information Technology." Therefore, MD 2.3 and MD 2.7 are eliminated.

This MD is subordinate to the requirements of the NRC Security Program as described in Volume 12 of the NRC Management Directive System.

TABLE OF CONTENTS

For updates or revisions to policies contained in this MD that were published after the MD was signed, please see the Yellow Announcement to Management Directive index (YA-to-MD index).

I. POLICY

A. It is the policy of the U.S. Nuclear Regulatory Commission (NRC) to ensure that reliable information technology (IT) infrastructure, unclassified (non-secure) telecommunications, and end user services are made available to agency staff and contractors in accordance with Federal statutes and regulations.

B. IT infrastructure, telecommunications, and end user equipment and services are acquired, engineered, implemented, operated, managed, and governed in accordance with Federal laws, regulations, circulars, and other applicable guidance.

C. Limited personal use of agency IT by NRC staff is permitted if the use does not interfere with official business, involves minimal or no additional expense to the NRC, or does not violate NRC ethical conduct requirements established by the Office of the General Counsel (OGC) in accordance with Federal laws, regulations, circulars, and other

applicable guidance. Guidance regarding what is, and what is not, allowed is provided in the NRC's "Agency-wide Rules of Behavior for Authorized Computer Use," which NRC users must sign upon joining the NRC, and thereafter as part of their annual computer security awareness training.

II. OBJECTIVES

- Design, acquire, and operate efficient, effective, and economical IT infrastructure (including telecommunications) and end user services that support NRC business needs and ensure accountability through the development and application of appropriate, cost-effective controls.
- Provide adequate and reliable computer, network, IT infrastructure, and support services that ensure the continued operation of the agency's operational, emergency, incident response, and contingency missions.
- Provide basic IT infrastructure and support services for the agency, including interaction with the public, licensees, vendors, and others outside of the agency.
- Provide computer and network capabilities and an IT infrastructure that are secure, robust, and responsive to changing business needs.
- Ensure that usage of NRC end user and IT infrastructure services adheres to the agency's IT architecture, applicable standards, criteria, codes, security controls, and requirements, and outlines acceptable conditions for the personal use of IT by NRC employees.
- Ensure that the NRC adheres to Federal statutes, regulations, policies, standards, procedures, and practices governing the appropriate management and use of IT.
- Provide guidance to agency staff and contractors on using NRC computer and network capabilities and IT infrastructure responsibly.

III. ORGANIZATIONAL RESPONSIBILITIES AND DELEGATIONS OF AUTHORITY

A. Executive Director for Operations (EDO)

The Executive Director for Operations (EDO) has inherent U.S. Government authority, must be a Government employee, and is responsible for the following as they relates to IT infrastructure and end user services programs:

1. Serves as the Chief Operating Officer, supervises the Chief Information Officer (CIO).

2. Reviews and approves the NRC IT/IM Strategic Plan (available at https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1908/), submitted by the CIO.

3. Delegates responsibility to the CIO to approve the Enterprise Architecture (EA) and Enterprise Roadmap, to include IT infrastructure and end user services.

4. Ensures that the statutory responsibilities regarding IT Investments and their oversight are appropriately assigned to the CIO.

5. Ensures that the NRC's planning and budgeting for IT investments are consistent and are integrated with the NRC's overall planning, budgeting, and performance management (PBPM) process.

6. Ensures that office and IT officials (applicable management staff or designees) participate in the planning and budgeting process for IT investments.

7. Designates the CIO as the Approving Official (AO)[1] to assume formal responsibility for approving the operation of an IT/IM system at an acceptable level of risk based on an agreed-upon set of implemented security controls, in accordance with the Federal Information Security Management Act of 2014 (Public Law 113-283), the E-Government Act (Public Law 107-347), and guidelines set forth by the National Institute of Standards and Technology (ML21137A147).

B. Chief Financial Officer (CFO)

1. In conjunction with the EDO, ensures that funds are available for the development and maintenance procedures to collect costs associated with the IT infrastructure and end user services programs.

2. Co-chairs the executive-level IT investment review board with the CIO.

3. Together with the EDO and CIO, reviews and approves the selections and budget for the IT investment portfolio recommended by the executive-level IT investment review board and submits recommendations to the Chairman, in accordance with the Federal Information Technology Acquisition Reform Act of 2014, commonly referred to as FITARA.

[1] Approving Official – This title was formerly referred to as the Designated Approving Authority (DAA). The DAA for major IT investments was composed of the Chief Information Officer (CIO), the Deputy Executive Director for Materials, Waste, Research, State, Tribal, Compliance, Administration, and Human Capital, and the Deputy Executive Director for Reactor and Preparedness Programs under the FISMA Act of 2002. The FISMA Act of 2014, which superseded the FISA Act of 2002, designates the CIO as the Approving Official for the NRC.

4. Ensures that IT investments are implemented, managed, and evaluated in accordance with Federal statutes and regulations by obtaining CIO approval of IT-related portions of the agency's investment submittals to the Office of anagement and Budget (OMB), Congress, and the Government Accountability Office (GAO).

5. Ensures that appropriate financial officials participate in the PBPM process for IT investments throughout their lifecycle.

6. Coordinates financial system plans with the CIO to ensure consistency with overall agency IT plans and architecture.

7. Maintains an inventory of the agency's capital assets, including internal use software that meets the requirements set by the Federal Accounting Standards Board in the Statement of Federal Financial Accounting Standard No. 10, "Accounting for Internal Use Software."

8. Establishes policies and procedures for accounting for internal use software development projects, and ensures that NRC staff comply with the guidelines for accounting for internal use software set by the Office of the Chief Financial Officer (OCFO).

C. Inspector General (IG)

Oversees and conducts audits and investigations of the NRC IT infrastructure and end user services programs to promote economy, efficiency, and effectiveness, and prevent and detect fraud, waste, abuse, and mismanagement.

D. Chief Information Officer (CIO)

The CIO has inherent U.S. Government authority, must be a Government employee, and is responsible for the following as they relate to IT infrastructure and end user services programs:

1. As delegated by the EDO, plans, develops, and oversees the agency's IT portfolio and IT investments.

2. Ensures compliance with Federal mandates and OMB guidance regarding the management of IT (e.g., FITARA and implementation of the Common Baseline for IT Management).

3. Co-chairs with the CFO the executive-level IT investment review board to lead the executive review function, as required by FITARA.

4. In conjunction with the CFO, provides yearly budget formulation guidance for IT investments.

5. Serves as the agency business line lead for all IT products.

6. In conjunction with the CFO, leads the executive-level IT investment review board's review of, and advises on, IT investment selections and budget for the agency's IT portfolio, and submits recommendations to the EDO. Advises the EDO, Chairman, and Commission throughout the overall PBPM process.

7. Establishes other executive and technical review or advisory bodies, as necessary, to involve office officials in IT investment planning and management oversight, ensures agencywide coordination, and supports compliance with the Capital Planning and Investment Control (CPIC) requirements for IT investments, EA, security, and information and records management, as stated in Part 7 of OMB Circular A-11, "Preparation, Submission, and Execution of the Budget," and OMB Circular A-130, "Managing Information as a Strategic Resource."

8. Ensures the implementation and operation of a reliable and effectively managed IT infrastructure and end user services that support the agency's computing and information management needs in delivering the NRC mission.

9. Establishes and maintains agencywide policies, architectures, and standards governing the agency's IT environment.

10. Approves all IT contracts, services, and purchases, or delegates authority consistent with the FITARA.

11. Approves submittals to OMB, Congress, and GAO related to IT investments, programs, and projects.

12. Reviews and concurs on the NRC IT/IM Strategic Plan and submits it to the EDO for approval.

13. Ensures agency compliance with Federal statutes, regulations, policies, standards, procedures, and practices governing the appropriate management and use of IT.

14. Establishes guidelines to ensure that limited personal use of Government-furnished IT does not interfere with official business and results in minimal or no additional expense to the NRC.

15. Ensures timely delivery of high-quality IT services through the implementation of an IT service model and effectively orchestrated processes and workflows between branches within and among all divisions within OCIO.

16. As the AO—

    (a) Assumes responsibility and is accountable through the system security authorization process for the security risks associated with an IT system.

    (b) Approves or disapproves security plans, memoranda of agreement or understanding, and plans of action and milestones.

    (c) Authorizes and deauthorizes IT system operations.

    (d) Halts operations of any IT system when it determines that an unacceptable level of risk exists.

    (e) Coordinates authorization activities with the Chief Information Security Officer (CISO), common control providers, information owners, system owners, security control assessors, and other interested parties during the security authorization process.

    (f) Determines the actions necessary to mitigate risks discovered during continuous monitoring, annual assessments, and penetration testing.

    (g) Authorizes significant system changes and determines if reauthorization is required.

    (h) Approves deviations from defined security requirements.

E. Deputy Chief Information Officer (Deputy CIO)

Approves requests for the repair, transfer, or disposal of IT hardware and software, network equipment, automated systems,telecommunications equipment, filing equipment and systems, micrographics equipment,library materials, and printing and copying equipment.

F. Chief Information Security Officer (CISO)

The CISO is responsible for the agency's Cybersecurity Program, including policy, procedures, and control techniques. The CISO has inherent U.S. Government authority, must be a Government employee, and is responsible for the following as they relate to the agency's IT environment:

1. Functions as the NRC risk executive and identifies the overall risk posture based on the aggregated risk from each of the information systems and support infrastructures for which the organization is responsible (e.g., security categorizations, common security control identification). This helps ensure consistent risk acceptance decisions.

2. Provides leadership input and oversight for all risk management and IT security activities across the agency.

3. Ensures the development and implementation of cybersecurity requirements, processes, procedures, standards, and templates for all IT efforts.

4. Ensures early identification and reporting of cybersecurity issues within the agency's IT environment.

5. Oversees IT efforts to identify cybersecurity risks.

6. Assesses risk and authorizes recommendations for IT implementations to the AO.

7. Oversees IT contingency planning for the agency.

8. Guides the maturation of the security processes within the NRC and advocates these concepts to NRC organizations.

G. Director, Office of Nuclear Security and Incident Response (NSIR)

1. Implements National Security and Emergency Preparedness (NS/EP) telecommunications procedures to support an effective response to public health and safety or environmental threats at NRC-licensed facilities.

2. Manages NRC, non-IT information security programs that specifically deal with the classification, declassification, and handling of classified information and safeguards information.

3. Ensures security, operation, and maintenance of NRC's classified computing capability, and acts as the owner of all classified information systems at the NRC.

4. Ensures IT infrastructure has secure operation of the classified communications center for organizational messaging and other classified transmissions.

5. Ensures the acquisition, distribution, and maintenance of classified phones, faxes, secure video teleconferencing, and other secure equipment and cryptographic keying devices.

H. Director, Office of Administration (ADM)

1. Serves as the senior agency official for the NRC Insider Threat Program.

2. Approves banner language for all electronic devices and computer networks to ensure compliance with Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," and the NRC Insider Threat Program.

3. Serves as a member of the executive-level IT investment review board and advises on IT acquisition planning and strategies.

4. As required by FITARA, in consultation with the CIO and the CFO, ensures all acquisitions that include IT are —

   (a) Led by personnel with appropriate Federal acquisition certifications, including specialized IT certifications, as appropriate;

   (b) Reviewed for opportunities to leverage acquisition initiatives such as shared services, category management, strategic sourcing, and incremental or modular contracting and use such approaches, as appropriate;

   (c) Supported by cost estimates that have been reviewed by the CIO; and

   (d) Implemented adequate incremental development.

5. As required by FITARA, ensures contract actions that contain IT are consistent with CIO-approved acquisition strategies and plans.

I. Chief Human Capital Officer (CHCO)

1. Serves as a member of the executive-level IT investment review board and advises on workforce planning and strategies.

2. As required by FITARA, in consultation with the CIO, develops a set of competency requirements for IT staff, including IT leadership positions, and develops and maintains a current workforce planning process to ensure the agency can accomplish the following:

   (a) Anticipate and respond to changing mission requirements.

   (b) Maintain workforce skills in a rapidly developing IT environment.

   (c) Recruit and retain the IT talent needed to accomplish the mission.

3. In conjunction with the CIO, identifies all positions within the agency that require the performance of IT specialist or other cyber-related functions and ensures the correct, corresponding employment code is assigned.

4. Aids in the development and delivery of the cybersecurity awareness and role-based training program for NRC IT users. Provides other IT-related training, as requested.

5. Maintains related training records for NRC IT users.

6. Maintains role-based training records for NRC personnel (for example, general users, system administrators, Information System Security Officers (ISSOs), and users with significant IT responsibilities).

7. Notifies the CIO of NRC staff terminations and transfers.

J. Office Directors and Regional Administrators

1. Ensure that NRC employees and NRC contractor personnel under their jurisdiction are aware of and comply with the provisions of this MD, as appropriate.

2. Provide the CIO, CFO, Deputy CIO, the executive-level IT investment review board, and management-level IT investment review board, and/or appropriate OCIO staff with information on office or regional IT investments, needs, and plans, as requested to support agencywide IT planning, budgeting, and investment control.

3. Ensure that IT investments are planned in consultation with, and approved by, the CIO before acquisition.

4. Ensure IT commodities are purchased through OCIO's centralized IT purchasing process.

5. Ensure that the implementation of IT (e.g., hardware, software, and firmware) be authorized by the CIO before it is used for NRC purposes or connected to NRC resources.

6. Ensure participation of business subject matter experts in the IT strategic planning process.

7. Define the requirements needed to support the business needs of the office or region. When existing IT capabilities no longer meet the business need and/or for opportunities for improvements or innovation, ensure new or changing business needs are submitted through OCIO's intake process to initiate OCIO engagement in finding the appropriate solution for NRC's IT environment.

8. Initiate administrative actions to collect charges incurred for unauthorized usage where appropriate and economically feasible, in accordance with OMB Circular No.A-123.

9. Ensure that all local, unclassified telecommunications systems are properly documented and accredited as stipulated under the Federal Information Security Management Act (FISMA).

10. For office/region-specific IT investments –

    (a) Designate a qualified project manager to coordinate the resources, funding, and business impacts for the sponsoring office and to perform the day-to-day operational activities to ensure that the investment is implemented in accordance with this MD.

    (b) Submit all project plans, management approaches, IT budget requests, and budget execution change requests to OCIO through the CPIC and IT budget processes for CIO approval.

    (c) Certify that the system security controls listed in the system security plan have been assessed using the methods and procedures described in the system security test and evaluation plan and the contingency plan, are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements for the system.

    (d) Certify for decommissioned systems that the approved system decommissioning process was followed as explained in current agency cybersecurity policy, and that the system is no longer being used by the NRC.

K. Director, Division of Resource Management and Administration (DRMA), Office of the Chief Information Officer (OCIO)

1. Oversees the agencywide IT/IM business lines budget formulation and execution activities.

2. Manages the formulation of the agency's IT/IM budget for submission to senior agency management and the CFO.

3. Oversees the development of IT/IM budget-related deliverables consistent with requirements of the agency leadership, Commission, and OMB.

4. Maintains the agency's IT/IM budget data, facilitates execution year change requests, and manages the purchasing agents and process for making centralized IT/IM purchases for the agency.

5. Manages OCIO's IT/IM budget execution including, funding IT/IM contracts, reviewing commitment and spending activities, and providing budget planning, acquisition and oversight.

6. Oversees budget execution and formulation and related performance reporting requirements for OCIO.

7. Provides advice and assistance in connection with the execution and administration of OCIO contracts.
8. Coordinates quarterly performance plan reviews and oversight of internal controls.
9. Leads the coordination of strategic workforce planning for OCIO in accordance with agency policy and guidance established by the CHCO.
10. Oversees all aspects of human capital management for the office, including the development of a staffing strategy and plan to ensure that core critical skills are maintained.

L. Director, Governance and Enterprise Management Services Division (GEMSD), Office of the Chief Information Officer (OCIO)

1. Oversees the development and implementation of the IT/IM Strategic Plan.
2. Oversees the development of NRC's cloud strategy and enterprise architecture, including its cloud architecture.
3. Ensures the agency's IT/IM investments, capabilities, and plans are continuously aligned with and prioritized by the agency's mission requirements.
4. Ensures effective governance and adoption of IT products and technological solutions and manages the Technical Reference Model.
5. Ensures the agencywide IT/IM investment performance and reporting to OEDO and OMB.
6. Manages the agency's CPIC policy and processes and leads and coordinates the implementation of Technology Business Management (TBM) services and reporting.
7. Ensures proper coordination with the Financial Management Branch in DRMA, OCIO, to ensure that investments align with TBM requirements and agency needs.
8. Establishes the IT project delivery lifecycle processes and program and project management methods, reporting, and tools.
9. Manages cybersecurity and enterprise architecture-related audits and data calls with the Office of the Inspector General and GAO, and reports compliance information to OMB, Department of Homeland Security, and other agencies.
10. Manages information security-related efforts, including managing and implementing the Controlled Unclassified Information program.
11. Ensures compliance with laws, regulations, and principles of fiscal integrity.

12. Determines measures to reduce costs where appropriate.

13. Oversees a range of IT planning and architecture, and a variety of cross-cutting operational, organizational services to support enterprise platform services.

14. Develops guidance in planning new platform services, including valid cost estimates for future support and maintenance.

15. Manages the lifecycle of official agency records and the implementation of NRC's Freedom of Information Act (FOIA) and information collections programs.

16. Participates in, and advises on, strategic workforce planning and ensures proper staff development to maintain an IT workforce capable of delivering essential IT services to support the agency's mission in a rapidly changing environment.

M. Director, IT Service Development and Operations Division (SDOD), Office of the Chief Information Officer (OCIO)

1. Oversees a number of IT investments. For each IT investment—

   (a) Designates a qualified project manager to coordinate the resources, funding, and business impacts for the sponsoring office and to perform the day-to-day operational activities to ensure that the investment is implemented as described in this MD.

   (b) Submits all project plans and management approaches to OCIO/GEMS through the CPIC processes for CIO approval.

   (c) Submits all IT budget requests and budget execution change requests to OCIO/DRMA through the IT budget processes for CIO approval.

   (d) Certifies that the system security controls listed in the system security plan have been assessed using the methods and procedures described in the system security test and evaluation plan and the contingency plan, are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements for the system.

   (e) For decommissioned systems, certifies that the approved system decommissioning process was followed as explained in current agency cybersecurity policy, and that the system is no longer being used by the NRC.

2. Provides subject matter expertise to inform the IT/IM Strategic Plan and IT Roadmap.

3. Provides day-to-day support to keep agency IT infrastructure secure, operational, and available.

4. Provides end user hardware, software, logistics, and services in support of enabling end user IT requirements.

5. Implements NRC's cloud and data center optimization strategies.

6. Manages the development, testing, and operations and maintenance of both Commercial Off-the-Shelf and NRC enterprise applications.

7. Unifies development and operations to achieve accelerated and more frequent deployment of changes to production.

8. Manages information security operations, including the Security Operations Center.

9. Manages the network operations, including the Network Operations Center.

10. Manages the data center, telecommunications, and system (i.e., server, operating system, database, application, etc.) operations.

11. Ensures enhanced coordination between IT services and other IT/IM functions to accelerate delivery.

12. Manages on-premise and cloud-based IT infrastructure, platforms, systems, applications, and the related end user services in a manner that accelerates delivery and increases efficiency and reuse.

13. Participates in, and advises on, strategic workforce planning and ensures proper staff development to maintain an IT workforce capable of delivering essential IT services to support the agency's mission in a rapidly changing environment.

N. Director, Division of Facilities and Security (DFS), Office of Administration (ADM)

1. Ensures that appropriate buildings and rooms are provided for NRC IT systems, and participates in planning, installation, and operation and maintenance of those buildings and rooms.

2. Coordinates, reviews, and approves, in conjunction with OCIO, physical security proposals and plans for buildings and rooms that will be used for processing NRC electronic information.

3. Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC personnel security program, including clearing personnel so that system owners can authorize their access to NRC IT systems.

4. Administers the NRC Insider Threat Program in coordination with other designated NRC offices.

5. Plans, develops, establishes, and administers policies, standards, and procedures for the overall NRC Facility Security Program including the review, survey, and approval of facilities and spaces for handling, receiving, storing, transmitting, processing, and protecting of classified, controlled unclassified information, and safeguards data and information.

6. Administers and issues Personnel Identity Verification cards to comply with Homeland Security Presidential Directive 12, “Policy for a Common Identification Standard for Federal employees and Contractors.”

7. Conducts surveys and approves spaces that receive, process, transmit, or protect classified data or information including non-NRC facilities that handle classified, controlled unclassified information, and safeguards data and information

8. Develops and implements NRC’s property management program that includes receipt, management, and disposal processes for IT assets.

9. Destroys sensitive IT equipment.

10. Reviews and approves all security plans for foreign assignees in accordance with MD 12.1, “NRC Facility Security Program.”

O. Director, Acquisition Management Division (AMD), Office of Administration (ADM)

1. Ensures that Federal and NRC requirements for information protection, system availability, and continuity of operations, as documented in Volume 12, “Security,” of the NRC MD catalog, are included in solicitations and contracts for the design, development, acquisition, or operation and maintenance of IT systems.

2. Implements and enforces acquisition processes that comply with requirements mandated by FITARA and associated guidance issued by OMB.

IV. APPLICABILITY

A. The policy and guidance in this MD apply to all NRC staff, and NRC contractors to whom they apply as a condition of a contract or a purchase order.

B. Unless otherwise specified, this MD covers policy and guidance for acquiring and using NRC’s IT infrastructure resources, including IT applications and hardware maintained by other offices.

V. DIRECTIVE HANDBOOK

Directive Handbook 2.6 provides guidelines and procedures for the acquisition, management, maintenance, and appropriate usage of NRC IT infrastructure and end user services.

VI. REFERENCES

Code of Federal Regulations

Federal Acquisition Regulations (FAR) (Title 48 CFR, Chapters 1 and 20).

"Scope of the Combined Federal Campaign (5 CFR 950.102).

"Standards of Ethical Conduct for Employees of the Executive Branch" (5 CFR 2635).

Executive Orders

Executive Order 13618, "Assignment of National Security and Emergency Preparedness Telecommunications Functions."

Executive Order 12656, "Assignment of Emergency Preparedness Responsibilities."

Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."

Federal Accounting Standards Board

Statement of Federal Financial Accounting Standard No. 10, "Accounting for Internal Use Software."

Federal Emergency Management Agency

Federal Executive Branch Continuity of Operations (COOP), June 15, 2004.

General Services Administration

Federal Standard 1037C, "Telecommunications Glossary of Telecommunication Terms."

General Services Administration (Federal CIO Council), "Recommended Executive Branch Model Policy/Guidance on 'Limited Personal Use' of Government Office Equipment Including Information Technology," May 19, 1999.

National Archives and Records Administration

National Archives and Records Administration General Records Schedule 12.

National Communications System Directives

National Communications System (NCS) Directive 2-1, "Plans, Programs, and Fiscal Management—National Security and Emergency Preparedness (NS/EP) Telecommunications Planning Process."

NCS Directive 3-1, "Telecommunications Operations—Telecommunications Service Priority (TSP) System for NS/EP."

NCS Directive 3-3, "Telecommunications Operations—Shared Resources (SHARES) High Frequency (HF) Radio Program."

NCS Directive 3-4, "Telecommunications Operations—National Telecommunications Management Structure (NTMS)."

NCS Directive 3-8, "Telecommunications Operations—Provisioning of Emergency Power in Support of NS/EP Telecommunications."

NCS Directive 3-9, "Telecommunications Operations—Communications Resource Information Sharing Initiative."

NCS Directive 3-10, "Minimum Requirements for Continuity Communications Capabilities."

NCS Directive 4-1, "Technology and Standards—Federal Telecommunications Standards Program."

NCS Directive 4-3, "Technology and Standards—Interoperability of Telecommunications in Support of NS/EP."

National Institute of Standards and Technology

Federal Information Processing Standard 140-2, "Security Requirements for Cryptographic Modules."

National Security Agency

National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 101, "National Policy on Securing Voice Communications."

National Telecommunications and Information Administration

National Telecommunications and Information Administration, "Manual of Regulations and Procedures for Federal Radio Frequency Management."

Non-Federal Guidance and Web Sites

ATIS Telecom Glossary 2007, published by the Alliance for Telecommunication Industry Solutions, 2007.

Building Industry Consulting Service International (https://www.bicsi.org/default.aspx).

National Fire Protection Association (http://www.nfpa.org).

Technology Business Management (https://www.tbmcouncil.org).

Telecommunications Industry Association (http://www.tiaonline.org).

Nuclear Regulatory Commission (NRC) Documents and Guidance

Information Technology Information Management Strategic Plan (https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1908/).

NRC Configuration Control Board (available in the NRC Service Catalog).

NRC Memorandum to David J. Nelson, Chief Information Officer, from Margaret M. Doane, Executive Director for Operations, U.S. Nuclear Regulatory Commission's Approving Official for Major Information Technology Investments; June 3, 2021 (ML21137A147).

NRC Service Catalog (access from the NRC Intranet home page or by the desktop icon on all standard NRC workstations).

NRC Memorandum to L. Joseph Callan, Executive Director for Operations, from John C. Hoyle, Secretary; Staff Requirements—COMNJD-98-003—NRC Staff Office Procedures; May 18, 1998 (ML003753754).

NRC Mobility Policy (ML17160A389).

OCIO Organization and Fuctions, available at https://www.nrc.gov/about-nrc/organization/ociofuncdesc.html.

OCIO Procedures, available at https://usnrc.sharepoint.com/teams/OCIOCommunications/Lists/OCIOProcedures/AllItems.aspx.

OCIO Service Model, available at https://usnrc.sharepoint.com/teams/OCIOServiceModel/SitePages/Overview.aspx?cid=1c434014-f3bb-4139-8d2e-015def6511e8.

OCIO Service Ownership Hub, available at https://usnrc.sharepoint.com/teams/OCIOServiceModel/SitePages/Overview.aspx.

OIG Hotline, available at https://www.nrc.gov/insp-gen/oighotline.html.

"U.S. Nuclear Regulatory Commission Agency-wide Rules of Behavior for Authorized Computer Use," September 19, 2017 (ML17244A084).

Management Directives (MDs)

MD 1.1, "NRC Management Directives System."

MD 2.8, "Integrated Information Technology/Information Management (IT/IM) Governance Framework."

MD 3.53, "NRC Records and Document Management Program."

MD 5.13, "NRC International Activities, Practices, and Procedures."

MD 7.4, "Reporting Suspected Wrongdoing and Processing OIG Referrals."

MD 8.2, "NRC Incident Response Program."

MD 10.162, "Disability Programs and Reasonable Accommodation."

MD 11.1, "NRC Acquisition of Supplies and Services."

MD 11.7, "NRC Procedures for Placement and Monitoring of Work with Federal Agencies and U.S. Department of Energy Laboratories."

MD 12.1, "NRC Facility Security Program."

MD 12.4, "NRC Communications Security (COMSEC) Program."

MD 12.5, "NRC Cybersecurity Program."

MD 13.1, "Property Management."

Office of the Attorney General

The Attorney General, Office of the Attorney General Memorandum to the Heads and Inspectors General of Executive Departments and Agencies, "Procedures for Lawful, Warrantless Monitoring of Verbal Communications," May 30, 2002 (http://www.justice.gov/ag/readingroom/ag-053002.pdf).

Office of Management and Budget (OMB)

OMB Circular A-11, "Preparation, Submission, and Execution of the Budget."

OMB Circular A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control."

OMB Circular A-130, "Managing Information as a Strategic Resource."

OMB Memorandum M-05-16, "Regulation on Maintaining Telecommunication Services during a Crisis or Emergency in Federally-owned Buildings."

OMB Memorandum M-08-05, "Implementation of Trusted Internet Connection."

Presidential Directives

Presidential Policy Directive 8 (PPD-8), "National Preparedness."

HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors."

United States Code

The Clinger-Cohen Act of 1996 (40 U.S.C. 11101 et seq.).

The E-Government Act of 2002 (Public Law 107-347).

Freedom of Information Act (5 U.S.C. 552).

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

Federal Information Technology Acquisition Reform Act of 2014 (FITARA) Pub. L. 113-291.

Federal Personal Property Management Act of 2018 (Public Law 115-419).

The Inspector General Act (5 U.S.C.).

Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.).

The Privacy Act of 1974 (5 U.S.C. 552a).

Public Buildings, Property, and Works (Public Law 107-217; Title 40 U.S.Code).

Rehabilitation Act of 1973 (29 U.S.C. 701).

Telecommunications Accessibility Enhancement Act of 1988 (Public Law 100-542).

The Telecommunications Act of 1996 (Public Law 104-104).

U.S. NUCLEAR REGULATORY COMMISSION MANAGEMENT DIRECTIVE (DH)

DH 2.6	INFORMATION TECHNOLOGY INFRASTRUCTURE AND END USER SERVICES	DT-21-13
Volume 2	Information Technology	
Approved By:	Daniel H. Dorman Executive Director for Operations	
Date Approved:	December 9, 2021	
Cert. Date:	N/A, for the latest version of any NRC directive or handbook, see the online MD Catalog.	
Issuing Office:	Office of the Chief Information Officer IT Services Development and Operations Division	
Contact Name:	Rachel Johnson	

EXECUTIVE SUMMARY

Management Directive (MD) 2.6, "Information Technology Infrastructure," has been expanded and renamed, "Information Technology Infrastructure and End User Services."

This MD includes, and updates previous guidance found in MD 2.3, "Telecommunications," and MD 2.7, "Personal Use of Information Technology." Therefore, MD 2.3 and MD 2.7 are eliminated.

This MD is subordinate to the requirements of the NRC Security Program as described in Volume 12 of the NRC Management Directive System.

TABLE OF CONTENTS

For updates or revisions to policies contained in this MD that were published after the MD was signed, please see the Yellow Announcement to Management Directive index (YA-to-MD index).

I. INTRODUCTION

A. Information Technology (IT) changes rapidly. The U.S. Nuclear Regulatory Commission (NRC) strives to keep current with proven technologies to provide the agency with a secure and reliable IT infrastructure and IT capabilities that increase productivity and maximize value for the cost. To be in a better position to provide quality IT services to the agency, the Office of the Chief Information Officer (OCIO) has adopted an agile approach to procuring, developing, maintaining, and delivering IT. OCIO has moved away from a large seat contract with a single vendor for the agency's IT needs, to owning and managing its IT assets and overseeing multiple vendors to deliver IT services. This approach provides the agency with more agility and more transparency into cost and value in alignment with the Federal Information Technology Acquisition Reform Act of 2014 (FITARA) and Technology Business Management (TBM)(a methodology used to evaluate and communicate the overall value of IT to agency stakeholders). In conjunction with the implementation of an IT service model closely aligned with TBM, it also enables continuous service improvement with a focus on improving the customer experience.

B. While this handbook provides high-level guidance on the NRC's IT infrastructure (including unclassified telecommunications since it is largely provided over the network) and end user services delivered to all NRC users under its IT service model, details on NRC's IT service model, service area managers, and service owners is maintained on the OCIO Service Ownership Hub. In addition, guidance on current service offerings and processes for obtaining them is maintained online in the NRC Service Catalog accessible from the NRC Intranet home page or by double-clicking on the NRC Service Catalog icon on the desktop of all NRC-issued workstations.

C. Current guidance on the use of IT infrastructure and end user services outlined in this handbook is kept current by updating the "U.S. Nuclear Regulatory Commission Agency-wide Rules of Behavior for Authorized Computer Use" (ML17244A084) (hereafter referred to as the "NRC Rules of Behavior"), as needed. The NRC Rules of Behavior are provided to new employees as part of the onboarding process and are part of the required annual cybersecurity awareness training. Any revisions to the NRC Rules of Behavior are communicated to NRC staff by a Yellow Announcement. The NRC Service Catalog, the OCIO Service Ownership Hub, and the NRC Rules of Behavior are dynamic sources of information and, therefore, are considered the current guidance.

II. OCIO SERVICE MODEL

A. To support the transition to multiple vendors for various IT services and NRC's implementation of FITARA and TBM, OCIO established the OCIO Service Model to orchestrate and manage the delivery of IT services to its customers, both internal and external to the agency. Management Directive (MD) 2.6 addresses only IT services made available to all NRC employees and contract personnel to meet basic business requirements common to all users. While outside of the scope of this MD, the OCIO Service Model comprises all IT services delivered by OCIO to all its customers.

B. The OCIO Service Model packages all the technologies, processes, and resources across IT that are needed to deliver a specific business outcome while hiding technical complexity to make it easier for customers to get what they need in an easy and efficient manner. Adopting an end-to-end IT service model improves IT conversations with business partners while simplifying activities within IT.

C. Delivering seamless end-to-end services depends on the close collaboration between branches across OCIO with dependent functions supporting the various IT services. To better support the delivery of quality services seamlessly to the customer, OCIO has adopted an IT service model that stresses service ownership. The OCIO Service model differs from the OCIO organizational model because there are unique roles and responsibilities outside of the organizational responsibilities. For information on the IT

service model, including service areas and available services, visit the OCIO Service Ownership Hub.

D. Overall, each branch is expected, for the technical areas of their responsibility, to—

1. With guidance and support from GEMSD, provide necessary information for Capital Planning and Investment Control (CPIC) reporting on their investments, and develop, maintain, and execute project plans according to NRC's project management guidance within the agency's project management tool (currently PMM 2.0).
2. Develop, maintain, and execute communications plans, including communications to relevant agency stakeholders, for their areas of implementation. Communication plans must align with the overarching OCIO communication strategy set by DRMA.
3. Ensure appropriate policy, standards, governance, and training related to functional areas are developed and delivered based on applicable law and regulations and, when appropriate, industry best practices.
4. Identify and recommend new technology and/or business process changes, transformations, and innovations to increase efficiencies, reduce duplication, fill gaps, and enhance capabilities.
5. Support development of staff.
6. Serve as a service area manager (SAM) over the primary services provided by their branch.
7. Provide appropriate service delivery for their services areas, including—
   (a) Managing service requests and
   (b) Working with other branches, SAMs, and service owners to ensure appropriate levels of service.

III. SERVICE AREA MANAGERS (SAM)

A. A SAM is accountable for a portfolio of related services and keeps them aligned with the overall service strategy. A SAM provides service delivery leadership for a collection of services in a specific service area. OCIO maintains a list of current SAMs at the OCIO SAM and Service Owners.

B. A SAM's responsibilities are to—

1. Define the approach for managing services in their service area, including—
   (a) Defining the direction for the services and setting technical direction,
   (b) Identifying gaps in the portfolio of services,

(c) Prioritizing resources and projects supporting the services, and

(d) Representing the service area in strategic planning and roadmap development.

2. Provide leadership in addressing common challenges across services and promoting continual service improvement.
3. Collaborate with other SAMs and service owners to promote service alignment and quality.
4. Serve as a point of escalation for service area challenges and partner in identifying and engaging in opportunities for improvement.
5. Serve as a point of escalation for alignment between service owners and process owners.
6. Advise service owners on individual service level agreements (SLAs) and operating level agreements (OLAs), where applicable.
7. Provide quarterly briefings to the CIO, Deputy CIO, and OCIO Leadership Team on the status of their service areas, including on the performance of services with their service area.

IV. SERVICE OWNERS

A. A service owner is accountable for delivering a high-quality service for their customers within the agreed upon service levels. OCIO maintains a list of current service owners at OCIO SAM and Service Owners.

B. A service owner's responsibilities are to—

1. Track and manage performance of services and report status to key stakeholders.
2. Provide leadership and planning for defined customer service offerings.
3. Provide and maintain service information in the NRC Service Catalog and provide support procedures to the help desk.
4. Provide effective and timely communications, and training (self-help guides or videos, demonstrations, user training sessions, etc.) when applicable, on new or changes to services.
5. Report status and health of services to the SAM and OCIO leadership.
6. Monitor service support queues and manage them appropriately.
7. Manage and communicate on planned and unplanned service outages.
8. Engage customers in requirements gathering and in establishing SLAs, when applicable.

9. Review feedback and drive continual service improvement.
10. Work with performance metrics team to define and manage service metrics to ensure data collection and analysis allows for data driven decisions to improve services and customer experience.
11. Analyze service performance data to inform the service improvement plan.
12. Collaborate with other service owners to create OLAs.
13. Maintain awareness of, and abide by, IT Service Management (ITSM) Roles and Responsibilities.

V. PROCESS OWNER

A. The process owner is accountable for managing the ITSM processes that enable service delivery without being burdensome.

B. The process owner's core responsibilities are to—

1. Define processes and procedures for ITSM areas, such as Incident, Problem, and Change Management.
2. Define process objectives and establish leading practice workflows with feedback from service owners.
3. Maintain a process that is fit for the purpose and is executed as intended.
4. Own the sponsorship, design, and adaptations of the process and its metrics.
5. Keep service owners updated on ITSM process initiatives.
6. Track and manage process performance and drive process improvement.
7. Determine key performance indicators for the process and measure process performance through continual metrics analysis.
8. Work with other process owners, as needed, to promote streamlined service delivery.
9. Review, approve, and communicate process changes and improvements, and research and recommend ITSM tool enhancements or transitions.
10. Advise management of process breaches or deviations.
11. Document and communicate the processes they own.

    Note: These internal processes enable the efficient and effective delivery of IT services; they are not external facing (i.e., visible to the customer). Customer-facing procedures, including how to request certain IT services, can be found in the NRC

Service Catalog. OCIO/DRMA also maintains a set of office instructions, as appropriate. (See OCIO Procedures.)

VI. KEY BRANCHES OUTSIDE THE OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO)

A. Chief, Facilities Operations and Space Management Branch (FOSMB), Division of Facilities and Security (DFS), Office of Administration (ADM)

1. Develops and implements property management policy, processes, and procedures for the agency.
2. Develops and administers the agency's property management program, including records and inventory, and redistribution and disposal.
3. Ensures compliance with Federal property management policies and regulations.
4. Oversees NRC equipment through inventory programs.
5. Conducts necessary inventories for headquarters Government-furnished equipment and gives its findings to OCFO.
6. Manages the NRC warehouse operation.

B. Regional Chiefs, Information Resources Branch/Information Technology Branch (IRB/ITB), DRMA

1. Each region has a Chief, IRB/ITB, DRMA, who is responsible for overseeing IT and telecommunication services (including application/system development, end user support, and LAN administration) in accordance with OCIO guidance and alignment with the IT Strategic Plan, available at https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1908/.
2. Coordinates with OCIO on the purchasing of IT commodities and executes IT purchasing through regional purchasing agents, when applicable.

VII. INFORMATION TECHNOLOGY INFRASTRUCTURE AND END USER SERVICES: AVAILABLE SERVICES, SUPPORT, AND MAINTENANCE

A. IT infrastructure services provide the core infrastructure required to deliver any technology automation. In general, these services are not customer-facing, or directly consumed by users, but rather enable the delivery and use of end user services that are directly consumed by users. IT infrastructure services include a logical collection of related services under the following service areas:

1. **Compute Services** includes all the physical and virtual computing services that run business applications, software tools, and system services. These compute services can be dedicated or on-demand and may be located on-premises or through external managed services or cloud offerings.

2. **Data Center Services** include the various facility services that provide a secure and controlled environment for housing compute, storage, network, and other technology equipment. In addition to the main data center at headquarters and the failover site at the designated region, data center services include smaller, secured rooms and telecom closets at NRC facilities.

3. **Network Services** include the voice and data networks, and supporting services such as load balancing, domain services, virtual private network (VPN), Intranet, and the Internet to enable communications within and outside the agency.

B. Storage Services include the various offerings for persisting information, data, files, and other object types (ex. Recordings/video). The service offerings range from supporting real-time, high-performance data retrieval to slower retrieval to long-term archive storage. DIfferent storage offerings (e.g. online backup, offline media, cloud storage) affect how current your backup data is and how long the restoration process takes. The choice of storage offerings is based on the business requirements for recovery in the event of data loss or a storage failure.

C. End User Services include the client computing devices, software, and connectivity to enable the workforce to access business applications; to communicate with other employees, partners, and customers; and to create content using productivity software. Direct user interaction or interface is provided under the following service areas:

1. **Client Computing Services** includes all the physical and virtual devices and associated services that enable a user to interact with the agency's IT systems. Examples of client computing devices include desktops, laptops, mobile devices, and virtual desktop environments.

2. **Communication and Collaboration Services** include the services that allow an end user to communicate with other people by e-mail or chat, to collaborate through shared workspaces, and to create and print content such as documents, presentations, videos, and other forms.

3. **Connectivity Services** include the network access services that provide a user access to the agency's technology systems. This includes wired and wireless access while on the premises and remote access while offsite.

D. The NRC provides an agencywide IT infrastructure and end user services for official, authorized, and limited personal use by NRC employees. The NRC also provides IT infrastructure and end user services for official use by certain NRC contractors as a condition of a contract or a purchase order. Specifically, SDOD is responsible for the following:

1. Providing and maintaining basic agencywide IT infrastructure, end user, and related support services to each agency employee and contractor for whom it is a condition of a contract. Basic IT infrastructure and end user services include the following:

   (a) NRC workstation, which includes a laptop with a docking station, monitor, keyboard, mouse, and an office productivity suite;

   (b) Network access, both local and remote;

   (c) Individual cloud storage space;

   (d) Shared network storage space;

   (e) E-mail;

   (f) Access to network printers;

   (g) Telecommunication service (e.g., voice, voice mailbox, data and video transmissions); and

   (h) Government-furnished mobile devices (e.g., smartphones, tablets) to those in eligible roles, as stated in the NRC Mobility Policy (ML17160A389).

2. Configuring standard workstations for network and Internet access and installing the standard image with the standard suite of productivity software (word processing, presentation, and spreadsheet applications, as well as e-mail and calendar). Productivity software also is available through NRC's cloud tenant to enable a mobile workforce. Requests for installations, moves, upgrades, or removals of desktop configuration, software, or peripherals must be approved by OCIO or regional office IT support staff.

3. Maintaining the software and hardware provided as part of the agencywide infrastructure and end user services by monitoring for manufacturer-issued patches and updates, testing those updates, and applying them to all supported workstations, as appropriate. Information on the standard IT service offerings can be found in the NRC Service Catalog.

4. Providing services for obtaining and using the related IT infrastructure and end user services. These services include installation and removal, upgrades, moves, help desk support, hardware/software maintenance, telecommunication services, network access, and operations services; as well as OCIO-owned, IT hardware and software provided and maintained by other offices and regions.

5. Establishing and implementing procedures where only designated OCIO staff, regional IT support staff, or the designated contractor support provides installation/removal, upgrades, moves, help desk support, maintenance, network access, telecommunication services, and operations services to support the IT infrastructure at NRC headquarters and, as appropriate, at regional offices and the NRC's Technical Training Center. Regional IT offices provide additional infrastructure support for the regions and resident sites in consultation with OCIO.

6. Developing and maintaining specific information and answers to questions regarding how to obtain, use, and maintain specific services or for timely news and information regarding IT resources and services that are found in the NRC Service Catalog.

7. Managing the day-to-day operation of the agency's data center facilities and communication infrastructure, including personnel access, monitoring, power and cooling, and space management.

8. Planning, coordinating, and directing the execution of disaster recovery planning and testing; developing recommendations to improve disaster recovery plans, procedures, and assets.

9. Operating the agency's Change Configuration Board (CCB) and ensuring proper authorization and planning of changes to the production operating environment.

10. Providing support for agency space modernization activities.

11. Operating, maintaining, and supporting the agency's data networks (e.g., intranet, internet, virtual private network), telecommunications services (e.g., Voice Over Internet Protocol, local and long distance telephone services, voicemail, mobile device support, and telephone handsets), and the Network Operations Center and Security Operations Center.

12. Providing configuration management and monitoring of the data and telecommunications infrastructure.

13. Supporting the agency's high-performance computing capabilities.

14. Providing technical support for the operation of agencywide business applications to include platform as a service (PaaS) and infrastructure as a service (IaaS).

E. OCIO adheres to the mandates and policy set forth in MD 10.162, "Disability Programs and Reasonable Accommodations," by—

1. Implementing Section 508 of the Rehabilitation Act of 1973, as amended, regarding accessibility of electronic information when NRC develops, procures, maintains, and uses electronic IT.

2. Assisting NRC offices in evaluating IT procurements to ensure consideration of access by individuals with disabilities in accordance with Section 508 of the Rehabilitation Act.

3. Ensuring that NRC publications services meet appropriate guidelines and provide appropriate access to individuals with disabilities.

4. Providing and installing appropriate, and properly reviewed, IT and telecommunication equipment and software related to reasonable accommodation requests.

5. Ensuring all external Web sites are accessible for the public.

F. OCIO manages and supports agencywide IT infrastructure services to facilitate appropriate and efficient connectivity at the NRC. These services and systems include the following:

1. Voice over Internet Protocol (VoIP) Capability

   The combination of phones, computing devices, connectivity, and software tools that provide users with the ability to make and receive telephone calls over the internet using their NRC laptops. VoIP capabilities and services are part of the standard workstation configuration.

2. Local and Long Distance Phone Service (Including Facsimile)

   Allows NRC staff and contractors to make calls within a defined geographical area and to destinations outside the local service area. Long distance service is centrally managed by OCIO.

3. Wire/Cable Infrastructure Support

   Supports the transmission of voice, data, and video communications. Once a building telecommunications distribution system has been approved by OCIO, the regions may add additional capacity using the approved architecture. However, regions must seek approval from OCIO for exceptions to the agency cabling and wiring standards.

4. Voice Messaging System and Audio Teleconferencing Service

   Allows callers to leave voice messages and provides live exchange of information among local and remote NRC employees and contractors and other NRC stakeholders.

5. Cellular Service

   Allows NRC employees to make phone calls and access remote data from any location within the United States and, with special provisioning, international locations.

6. Priority Calling Services

   Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) are acquired through the National Communications System (NCS), which provides priority calling through the telephone network to support mission requirements during an emergency.

7. Toll-Free Service Telephone Numbers

   Allow the public, employees, and contractors to contact the NRC without charge.

8. Federal Relay Services

   Federal Government telecommunications service that is facilitated by the General Services Administration that enables equal communication access for Federal employees with hearing or speech disabilities.

9. Mass Notification Services

   Serves as a mobile receiver and transmitter for emergency communication.

10. Leased Lines and Virtual Circuits (Communications Links)

    Transport data across networks within and outside of the NRC.

11. Internet Access Services

    Provide both dedicated and switched access to the Internet in support of the agency mission.

12. Access to the NRC's local area and wide-area networks (LAN/WAN) is provided only to those who meet the security requirements and need access for the performance of their duties.

    (a) NRC users must have a "Q" or an "L" security clearance or a Section 145b waiver before access is granted.

(b) Contractor personnel must have a “Q” or an “L” security clearance or an IT Level I or II access authorization before access is granted. A user identifier (user ID) and associated passwords are required to access the LAN/WAN.

13. Any hardware/software that does not have a current Authority to Operate (ATO) requires testing and additional approvals before being allowed on the NRC network.

14. User IDs are issued to specific individuals. Sharing user IDs and passwords is not permitted. Requests for Direct Network Access (DNA) to Intranet file shares through the BYOD (bring your own device) application must be approved by the user’s supervisor or COR, and by OCIO.

15. All users must sign the NRC Rules of Behavior (ML17244A084) before remote access is granted.

16. Remotely install NRC-approved software to an agency laptop, tablet, or phone or provide a Virtual Machine to run more high-powered software. BYOD users access NRC cloud services and use a license, but no NRC software is installed on their personal device. This is the same for web application use for Office 365.

17. Use of shareware/freeware/evaluation copies of software is permitted in accordance with applicable copyright laws if it is determined that the software meets an agency business need. This requires submitting a request through the intake process to ensure that the software is tested to work with the current NRC standard image, is included in the TRM, and follows the appropriate security authorization process.

18. NRC employees may use laptop IT resources at offsite locations within the United States without notifying OCIO; however, the NRC employee must sign an NRC Form 119, “Custodial Receipt for Sensitive and Nonsensitive Personal Property,” accepting responsibility for the sensitive item. Note: International travel requires use of pre-approved international IT equipment. See MD 5.13 "NRC International Activities, Practices, and Procedures.”

19. The Customer Support Center help desk staff does not provide training in the use of applications.

VIII. USE OF IT INFRASTRUCTURE AND END USER SERVICE: GUIDELINES FOR USAGE

The following guidelines apply to all users of the NRC's IT infrastructure and end user services and resources.

A. Appropriate Personal Uses

1. This policy is applicable to NRC employees. NRC contract staff are required to follow the rules outlined in their contractual agreement. Use of the NRC's IT infrastructure constitutes consent to monitoring. A consent to monitoring warning banner is displayed on workstations and mobile devices at initial user sign on.
2. All NRC property, including computers, mobile desktops, social media accounts, mobile devices, e-mail accounts, Internet connection, phones, copiers, and other equipment that belongs to the Government is intended for official purposes. NRC employees have the responsibility to use NRC property, including property leased to the NRC, for approved purposes only. The current NRC Rules of Behavior for Authorized Computer Use permits employees to use agency computers and other equipment for non-official purposes on a limited basis. Employees are expected to follow the guidance for use of IT as outlined in the NRC Rules of Behavior (ML20162A026) that are reviewed and signed by employees each year at the completion of the mandatory computer security awareness training course.
3. Personal use is defined as an employee's activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. NRC employees are specifically prohibited from using agency IT to maintain or support a personal, private business. Examples of this prohibition include employees using an agency computer and Internet connection to run a travel business or an investment service. The ban on using agency IT to support a personal, private business also includes employee use of agency IT to assist relatives, friends, or other people in these activities. Employees may, however, make limited use of agency IT to, for example, check their Thrift Savings Plan or other personal investments, to seek employment, to communicate with a volunteer charity organization, or to file a Freedom of Information Act or Privacy Act request during their non-working hours (e.g., lunch break).
4. All social media usage must be conducted consistent with existing NRC Rules of Behavior governing NRC employees.

B. Inappropriate Personal Uses of Agency Information Technology

Following are examples of inappropriate personal uses of NRC IT. This list is not all-inclusive and additional information on other prohibited activities can be found in the NRC Rules of Behavior Policy (ML20162A026).

1. Any personal use that could cause congestion, delay, or disruption of service to any agency system or equipment. Examples of possible misuse include streaming live sporting events and downloading or sending non-work-related video, sound, or other large file attachments that can degrade the performance of the entire network.

2. Use of the agency systems as a staging ground or platform to gain unauthorized access to other systems.

3. Creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings, regardless of the subject matter.

4. Use of agency IT for activities that are illegal, inappropriate, or construed as justifiably offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others based on race, age, parental status, religion, color, sex, disability, national origin, or sexual orientation.

5. Use of NRC computing resources for fundraising activities (except for activities such as the Combined Federal Campaign), endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited political activity (e.g., sending e-mail messages endorsing partisan political groups or candidates for partisan political office).

6. Use of IT, including telephone or facsimile service, to create, download, view, store, copy, transmit, or receive sexually explicit or sexually oriented materials, or materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.

7. Use of IT for commercial purposes, fundraising activities (except as provided in 5 CFR 950.102, “Scope of the Combined Federal Campaign”), support of “for-profit” activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services), endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited political activity.

8. Use of IT for posting agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as an NRC employee, unless appropriate agency approval has been obtained or the employee uses an appropriate disclaimer.

9. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software or data that includes privacy information, copyright, trademark, or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data.

10. Any use of IT involving modification of agency equipment, including configuration changes or loading of personal software (i.e., any executable code, as opposed to data, document, e-mail, images, or spreadsheets, not provided by the Government). Guidelines regarding the use of software for agency business are provided in MD 12.5, "NRC Cybersecurity Program."

11. Any other activity that interferes with official duties.

12. Employees should report any instance of abuse, fraud, or other wrongdoing to the Office of the Inspector General (OIG) through the OIG Hotline.

IX. GLOSSARY

A. This section relies heavily on the technology business management (TBM) taxonomy that defines the IT services common to most, if not all, IT organizations. These definitions have been widely used across industry for many years; however, TBM is still in the early stages of being implemented across the Federal Government. Not every term listed is used directly in this management directive (MD), but is used in either the NRC Service Catalog or the OCIO Service Ownership Hub, which the handbook references. By including the definitions here, the intent is to help orient NRC users to the IT services provided to them through NRC's IT service model to meet the requirements outlined in this MD.

B. Key objectives of implementing an IT service model are to drive continuous service improvement and enhance customer experience. As NRC's IT service model continues to evolve, service areas and services as defined here may be adapted to better reflect the IT service areas and services that best support the specific business needs of the agency to deliver its mission. As the agency transforms and technologies change, the NRC Service Catalog and the OCIO Service Ownership Hub will be updated accordingly.

Application Support Services

Provide the ongoing operational activities required to keep the application or service up and running and provide Tier 2 and Tier 3 technical support to more complex or difficult user questions and requests. May also include minor development and validation of smaller application enhancements (e.g., minor changes, new reports).

Capacity Management Services

Ensure that IT resources are right-sized to meet current and future business requirements in a cost-effective manner. Take into account the expected demand from the business or consumer along with the availability and performance of existing capacity and projects future requirements. Occurs across data center, compute, storage, network, and other IT resources.

Capital Planning and Investment Control

The planning, development, and acquisition of a capital asset and the management and operation of that asset through its usable life after the initial acquisition. IT capital investments may consist of one or more assets that provide functionality in an operational (production) environment.

Client Computing

An end user service area that includes all the physical and virtual devices and associated services that enable a user to interact with the agency's IT systems. Examples include desktops, laptops, mobile devices, and virtual desktop environments.

Communication and Collaboration Services

Allow an end user to communicate with other people by e-mail or chat, to collaborate through shared workspaces, and to create and print content such as documents, presentations, and other forms.

Compute Services

All the physical and virtual computing services that run business applications, software tools, and system services. Can be dedicated or on-demand and may be provided on-premises or through external managed services or public cloud offerings.

Connectivity Services

The network access services that provide a user access to the agency's technology systems. This includes wired and wireless access while on premise and remote access while off site.

Continuous Service Improvement

A methodology used to improve overall quality of service by continuously collecting and analyzing performance data to make data-driven decisions on improving services and products.

Customer Experience

The customer's perceptions and related feelings caused by individual and cumulative effect of interactions with a supplier's employees, systems, services, or products.

Customer Experience Management

The practice of designing and reacting to customer interactions to meet or exceed their expectations, leading to greater customer satisfaction, loyalty, and advocacy.

Data Center Services

The various facility services that provide a secure and controlled environment for housing compute, storage, network, and other technology equipment.

Data Network

A selection of network connection offerings that enable direct data communications across the organization including its data centers, office buildings, remote locations, and partners and service providers (including public cloud service providers) without traversing the public Internet. Typically provides a greater level of performance, security, and control.

Design and Development Services

Provide the planning, design, programming, documenting, testing, and fixing involved in creating and maintaining a software product.

Deployment and Administration

The release management and software distribution services to deploy new and/or the most recent software version to the host servers or client computing devices. Also includes ongoing operating system support and patch management.

Development Services

All the services to plan, design, build, test and release new application software and services.

Domain Services

Provision of lookup capabilities to convert domain names into the associated Internet Protocol address to enable communication between hosts.

Employee Non-Work Time

Time when an employee is not otherwise expected to address official business. For example, an employee could use an NRC computer during off-duty hours (before or after the workday or during his or her lunch period).

End User Services

Client computing devices, software, and connectivity to enable the workforce to access business applications, to communicate and collaborate with other employees and internal and external stakeholders, and to create content using productivity software, These are also known as “user-facing” services (i.e., services visible or known to the user).

Enterprise Architecture (EA)

The strategic, business, and technology documentation of the current and desired relationships among business and management processes and IT of an organization. An EA includes the rules, standards, and systems lifecycle information to optimize and maintain the environment that the agency wishes to create and maintain through its IT portfolio. An EA must provide a strategy that enables the agency to support its current state and provides a roadmap for transition to its target environment. An EA defines principles and goals and sets a direction on issues like the promotion of interoperability, open systems, public access, end user satisfaction, and IT security.

Enterprise Infrastructure Solutions (EIS)

A comprehensive, solution-based, acquisition vehicle available through the U.S. General Services Administration to provide enterprise telecommunications and networking solutions for Federal agencies.

Event Management Services

Monitor resources and applications. Services that record the application programming interface calls and deliver logs and insights. Services that provide log data consolidation, reporting, and analysis to enable IT administrators and security personnel to understand asset utilization, user logins, and information access.

Information Technology (IT)

Any equipment or interconnected system of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This equipment includes personal computers and related peripheral equipment (e.g., printers), software, telephones, photocopiers, e-mail, Internet connectivity, and access to Internet services.

IT Services

The application of business and technical expertise to enable organizations in the creation, management, and optimization of or access to information and business processes. The IT services market can be segmented by the type of skills that are employed to deliver the service (design, build, run).

IT Service Desk (Customer Service Center)

A single point of contact to meet the support needs of users and the IT organization by providing end users with information and support related to IT products and services, usually to troubleshoot problems or provide guidance about products such as computers, electronic equipment, or software. IT service desk support may be delivered through various channels such as phone, Web site, instant messaging, or e-mail. This also includes IT knowledge management in the NRC IT Service Catalog, request fulfillment, and desk-side support.

IT Service Management

The incident, problem, and change management services necessary for IT to plan, deliver, operate, and control the IT services offered to its customers. Also includes the software tools and services for assessing, recording, and managing asset configurations, such as server settings or network router tables.

IT Training

Educational services to the agency's users on how to access and effectively use the agency's business application services and common productivity software and tools.

Infrastructure Services

The core infrastructure (including data center facilities, compute, storage, network, and telecommunications services) that are required to deliver any technology automation but typically are not directly consumed by users.

Information and Communication Technology (ICT)

Information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include, but are not limited to, computers and peripheral equipment, information kiosks and transaction machines, telecommunications equipment, customer premises equipment, multifunction office machines, software, applications, Web sites, videos, and electronic documents.

Internet

Telecommunication services using the public Internet to enable communications across the organization including its data centers, office buildings, remote locations, partners, and service providers. Virtual Private Networks (VPNs), Local Area Networks (LANs), and Wide Area Networks (WANs) are created to limit access and provide security.

Intranet

A local or restricted network that enables employees to securely communicate among each other, to store information, and to share information within an organization.

Load Balancing

Ability to optimize incoming application/workload requests through load balancing and traffic management to deliver high availability and network performance to applications.

Minimal Additional Expense

Causing little or no increase in cost to the Government, involving only normal wear and tear on equipment, and the expenditure of only small amounts of electricity, ink, toner, and paper. Other examples include making a few copies from a photocopier or printer, infrequent personal e-mails, and other limited use of the Internet for personal reasons. Brief telephone calls or short facsimile transmittals are acceptable.

Network Access

A set of connection services that enable users to access the agency's internal private network from their client computing device. Once connected, they can access agency business applications and information and can communicate and collaborate with other users on the network. Appropriate access to external applications and Internet sites is allowed.

Network Services

The voice and data networks and supporting services (e.g., load balancing, domain services, virtual private network, Intranet, Internet) that enable communications within and outside the agency.

Operations

The activities performed to monitor, support, manage, and run the IT environment for the agency, including capacity management, deployment and administration, event management, and IT service management. These typically are services provided behind the scenes and not directly user-facing.

Remote Access

A set of connection services that enable users to access the agency's internal private network from their client computing device when away from agency buildings. Once connected, they can access agency business applications and information and can communicate and collaborate with other users on the network.

Storage Services

Various offerings for persisting information, data, files, and other object types. The services offerings range from supporting real-time, high-performance data retrieval to slower retrieval to long-term archive storage. Different storage offerings also provide recovery point objectives to meet the business needs of an application based on a business impact assessment.

Support Services

Within an IT service model, these are the centralized services that directly support the end user community regarding their IT needs, including application support and service desk. The technical support is generally categorized as Tier 1, where an IT help desk answers general questions and solves basic issues; Tier 2, where moderate issues are elevated for in-depth technical support; Tier 3, where complex issues are elevated for engineering-level support; and Tier 4, when issues are elevated to the vendor or manufacturer of the IT product because the solution is not within the IT organizations control.

System Integration

Development services that link together different computing systems and software applications physically or functionally, to act as a coordinated whole. This can be accomplished across systems that reside within the enterprise's data centers and with solutions that reside in the provider's facilities.

Technology Business Management (TBM)

A value-management framework instituted by Chief Information Officers, Chief Technology Officers, and other technology leaders. Founded on the transparency of costs, consumption, and performance, TBM gives technology leaders and their business partners the facts they need to collaborate on business aligned decisions.

Testing

Testing services execute a program or application with the intent of finding errors or other defects. The investigations are conducted to provide stakeholders with information about the quality of the product or service and allow the business to understand the risks of software implementation. Testing may take multiple forms including functional, system, integration, performance, and usability.

Virtual Private Network (VPN)

A secure method to authenticate users and enable remote access to corporate systems. VPN can also isolate and secure environments in the data center across physical and virtual machines and applications.

Voice Network

Telecommunication offerings for voice circuits to deliver "plain old telephone service," Voice over Internet Protocol (VoIP) services and other advanced features including 800-services and automatic call distribution.