SUPPLEMENTAL DIRECTIVE

NNSA SD 200.1A

Approved: 06-12-25
Recertification Due: 06-12-30

INFORMATION RESOURCES MANAGEMENT

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of the Associate Administrator for Information Management and Chief Information Officer

CONTROLLED DOCUMENT
AVAILABLE ONLINE AT:
http://directives.nnsa.doe.gov

OFFICE OF PRIMARY INTEREST (OPI):
Office of the Associate Administrator for Information Management and Chief Information Officer

printed copies are uncontrolled

THIS PAGE INTENTIONALLY LEFT BLANK

INFORMATION RESOURCES MANAGEMENT

1. PURPOSE. This Supplemental Directive (SD) defines the authorities, requirements, and responsibilities for the management of information technology (IT), including national security systems (NSS), information systems, operational technology (OT), internet of things (IoT) devices, and the application of information policies within the National Nuclear Security Administration (NNSA). This SD delineates authorities delegated to the Associate Administrator for Information Management and Chief Information Officer (NA-IM) (CIO) by the Under Secretary for Nuclear Security and NNSA Administrator (Administrator) in Delegation Order No. NA-005.01, dated 2-11-2019. NA-IM will implement policy for the oversight of information resources that align with the requirements outlined in executive, congressional, and delegated authorities.

2. AUTHORITY. Selected authorities are identified within this section. See Attachment 5, References, for additional information and authorities.

   a. Department of Energy (DOE) Order (O) 200.1A Chg. 2 (LtdChg.), *Information Technology Management*, dated 08-11-23.

   b. Delegation Order No. NA-2019-NA005.01, dated 2-11-2019.

   c. 40 United States Code (U.S.C.) 11315, 11316 and 11319 (2021).

   d. 44 U.S.C. 3101, 3102, 3505-3507, 3510-3511, 3513, 3515, 3517, 3518, 3520, 3552-3559, 3561-3564, 3571-2, 3576, 3581-3583, and 3601-3606 (2021).

3. CANCELLATION. NNSA SD 200.1, *Information Resources Management*, dated 12-14-23.

   Cancellation of a directive does not, by itself, modify or otherwise affect any contractual obligation to comply with the directive. Contractor Requirements Documents (CRD) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

4. APPLICABILITY.

   a. Federal. This SD and its Attachments apply to all NNSA Federal entities that acquire, operate, maintain, or dispose of IT, including NSS, information systems, IoT devices, and OT.

   b. Contractors. Except for the equivalencies and exemptions in paragraph 4.d., the CRD, Attachment 1, and Attachments 2-5, set forth requirements that apply to site and facility management contracts. The CRD and Attachments 2-5 must be included in the management and operating (M&O) contracts and the subcontracts to the M&O contracts that manage information systems, including NSS, IoT devices, and OT. M&O contracts must include DOE Acquisition Regulation clause 952.204-77, *Computer Security*.

c. Systems. This SD applies to a broad range of technologies and uses statutory definitions with a recognition that modern technology does not always fit within a singular definition. NNSA must make risk-based decisions to manage technology using the best information and the most appropriate process available. This SD identifies those processes and responsibilities that are applicable to certain NSS, IoT devices, and OT.

d. Equivalencies/Exemptions.

(1) Equivalency. In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 U.S.C. sections 2406 and 2511, and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

(2) Exemption. This SD does not apply to the Sensitive Compartmented Information (SCI) IT and information systems located at NNSA sites. SCI systems must comply with Director of National Intelligence Directives and Orders and Executive Order 12333, *United States Intelligence Activities*, accordingly, as advised by the DOE Director of Intelligence and Counterintelligence. Nothing in this SD will alter or supersede the existing authorities of the Director of National Intelligence.

5. BACKGROUND. This SD describes requirements and responsibilities to ensure the appropriate management and oversight for the acquisition, operation, maintenance, and disposal of NNSA's information resources.

6. REQUIREMENTS. NNSA information resources consisting of IT (including NSS, information systems, IoT devices, and OT), must be acquired, operated, maintained, and disposed of consistent with NNSA mission needs and all statutory, regulatory, and DOE and NNSA Directive requirements.

7. RESPONSIBILITIES.

a. Associate Principal Deputy Administrator. Serves as the IoT device waiver authority.

b. Director, Office of Policy and Strategic Planning.

(1) Coordinates with NA-IM to ensure alignment with the planning phases of Planning, Programming, Budgeting, and Evaluation (PPBE) process.

(2) Conducts planning studies on information resources issues, including cybersecurity, as appropriate, in collaboration with NA-IM.

c. Associate Administrator for Information Management and Chief Information Officer.

(1) Uses enterprise architecture to conduct information resources management strategic planning in alignment with the PPBE process to align resources to NNSA mission requirements.

(2) Conducts IT portfolio management (ITPfM) to review and approve IT and information system investments, as appropriate, in accordance with the responsibilities outlined in DOE O 200.1A, and Office of Management and Budget (OMB) Circular A-11, *Preparation, Submission, and Execution of the Budget*, § 55, *Information Technology Investments*.

(3) Supports the development of policies and procedures for IT and information system investment management including project oversight, in coordination with the Associate Administrator for Partnership and Acquisition Services (NA-PAS).

(4) Ensures that the operation, management, and use of IT and information systems comply with applicable statutes, regulations, policies, and directives to meet NNSA mission requirements, in coordination with the cognizant NNSA Contracting Officer or Contracting Officer's Representative, as needed.

(5) Develops information management policies and procedures that increase program efficiency, improves the integrity, quality, and utility of information across NNSA, implements appropriate security and classification controls, and enables the trustworthy use of decision-making systems.

(6) Establishes, maintains, and enforces the governance of IT policies and processes to enable the secure sharing of information and the performance of IT services, including information assurance, discovery, accessibility, and dissemination (including unclassified IT and information system policy releasability) requirements.

(7) Develops and conducts performance measurement assessments and reviews to evaluate the use of information resources and makes recommendations, as necessary, to the Administrator.

(8) Develops a comprehensive IT investment and acquisition review process in accordance with DOE O 200.1A and DOE O 413.3B, ensuring adherence to the following parameters:

(a) Sits on the Energy System Acquisition Advisory Board (ESAAB) as a full member to provide guidance and gain insight into the IT and information system portions of major capital asset projects.

(b) Ensures acquisitions not subject to review by the ESAAB follow the appropriate investment and procurement approval process in Attachment 2.

(c) Ensures NNSA IT and information system investments are reviewed by the DOE Information Management Governance Board, as appropriate.

(d) Adheres to the requirements and processes of DOE O 413.3B for IT and information system investments based on the thresholds identified in that Order.

(e) Reviews all acquisitions and procurements for IT or IT services to determine compliance with National Institute of Standards and Technology (NIST) IoT standards and recommends approval of IoT device waivers, in accordance with the *IoT Cybersecurity Improvement Act of 2020*.

(9) Authorizes Program and Functional Offices to manage OT, as appropriate.

(10) Ensures applicable mobile device management procedures are implemented in a manner per DOE O 203.2, *Mobile Technology Management*, to reduce risks to an acceptable level while supporting mission requirements, incorporating authorization, accountability, monitoring, training, and reporting requirements for users.

(11) Establishes and chairs the NNSA IT Investment Review Board (IRB). As prescribed by DOE, reviews and approves proposed Major IT and information system investments that meet or exceed the thresholds established in Attachment 2.

(12) Serves on boards, committees, and other groups pertaining to the assigned NA-IM responsibilities. Represents the Administrator on matters regarding IT resources outside of NNSA.

(13) Establishes or uses existing governance bodies and processes to ensure information policies and systems, along with IT, align with NNSA objectives and do not pose any undue risk to NNSA. Entrusts the governance bodies with performing the functions of reviewing and analyzing information and IT investments, addressing issues, and elevating unresolved matters.

(14) Ensures that IT investments meet the *Government Performance and Results Act of 1993* (GPRA) and the *GPRA Modernization Act of 2010* performance goals and reporting requirements, as appropriate.

(15) Develops guidance to support telework, implements new and emerging telework technologies for enterprise use, and develops guidelines for

protecting government furnished equipment and personally owned equipment used to access NNSA information systems for purposes of telework.

(16) Approves information and communications technology and services supply chain risk management practices and processes, in accordance with SD 205.1, *Baseline Cybersecurity Program*.

(17) Develops policies for the use of Internet domains for NNSA networks.

(18) Promotes the use of enterprise purchasing agreements for commercial off-the-shelf IT products or capabilities to focus resources on efficient and effective supplier management, where applicable.

d. Deputy Administrator for Defense Programs. Develops and implements policies, processes, and procedures for federal and contractor acquisition, operation, maintenance, digital assurance, and disposition of national security systems under their cognizance that are needed for the operation of defense programs, including, but not limited to:

(a) Nuclear weapons IT involving equipment that is an integral part of a weapon or weapon system;

(b) High performance computing systems (HPC) and associated software running on HPCs that are critical to the fulfillment of the nuclear security mission; and

(c) Command, control, and communications systems integral for the safe and secure transport of special nuclear materials.

e. Associate Administrator for Partnership and Acquisition Services.

(1) Coordinates with NA-IM regarding reviews of IT and IT-related acquisition plans, strategies, cost estimates, contractual actions, memoranda of understanding, and interagency agreements that involve plan, contract, or agreement modifications or result in substantial changes to IT resources within the scope of NA-PAS' authority.

(2) Ensures procurement requests are supported by cost estimates that have been reviewed by NA-IM, or the appropriate program office. Ensures that NA-IM or the appropriate program office approves IT procurements, acquisitions, and major investments, and confirms that the acquisition strategies and plans are consistent with existing IT policies.

(3) Coordinates with NA-IM and the Associate Administrator for Management and Budget (NA-MB) to implement a NNSA-wide process to ensure that any procurement or acquisition that includes IT or IT-related systems, solutions, or services includes personnel with the appropriate federal acquisition certification on the integrated project team.

(4) Updates program guidance, in coordination with NA-IM, to ensure programs executed under DOE O 413.3B or DOE O 415.1B, *Information Technology Project Management*, include NA-IM as a voting member on all Critical Decision (CD) Gate review boards, and ensures NA-IM reviews and approves IT investments within each gate review.

(5) Ensures contracts or interagency agreements that include IT have NA-IM approval prior to execution or are consistent with the acquisition strategy and plan approved by NA-IM.

f. Associate Administrator for Management and Budget.

(1) Updates and issues the NNSA Planning, Programming, and Fiscal Guidance in coordination with the Office of Cost Estimating and Program Evaluation, to include expenditures for investments in IT. Ensures budget requests including IT investments are reviewed and approved by NA-IM prior to submission to OMB.

(2) Provides the annual IT training and workforce certification requirements.

(3) Develops and implements workforce strategies and proficiency standards to ensure that the IT management, computer engineering, data science, and security administration position personnel possess the knowledge, skills, and abilities to meet the requirements of the job category including obtaining the appropriate certifications, as relevant to the position.

(4) Coordinates with NA-IM to ensure cybersecurity workforce strategies are in alignment with the NIST Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity*.

(5) Develops and implements procedures necessary to recruit and retain cybersecurity professionals according to OMB Memorandum (M)-16-15, *Federal Cybersecurity Workforce Strategy*, and the U.S. Office of Personnel Management guide, *Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals*.

g. NNSA Program/Functional Offices.

(1) Plan, program, budget, and execute IT investments, to include the acquisition, operation, maintenance, development, and disposal of the IT, unless otherwise required by policies or procedures.

(2) Review, approve, and report budget requests containing information system and IT resources to NA-IM in accordance with the process outlined in Attachment 2. Program and Functional offices must:

(a) Request an authorization assignment from NA-IM for the IT investment under program office or functional office responsibility.

ITPfM investments attributed to a program office that has not requested authorization assignments must be managed by NA-IM.

(b) Ensure IT investments, including IoT device and OT procurements, align with the mission of NNSA and applicable IT and cybersecurity requirements to include appropriate network architectures and technology standards.

(c) Ensure IT investments comply with Attachment 3, as appropriate.

(d) Ensure reviews and assessments are performed for IT, including IoT device and OT procurements, under their cognizance. Ensure proper reporting for IT procurements and investments.

(e) Consult with the appropriate Authorizing Official (AO) regarding applicable cybersecurity requirements if the technology is expected to connect to a NNSA network or to the internet directly. Procurement expenditures that involve equipment that will be operated within, connected to a cybersecurity accreditation boundary, or will be connected to a network must be reported to the Enterprise AO.

(f) Submit procurements and acquisitions for IT or IT services to NA-IM for review as well as requests for IoT device waivers when IoT devices do not comply with *IoT Cybersecurity Improvement Act of 2020* standards and guidelines.

(3) Ensure all proceedings by a Program Office IT IRB, or similar IT governance board, are sent to NNSA-OCIO-FITARA@nnsa.doe.gov.

(4) Develop a plan, in coordination with NA-IM, that requires OT to be managed throughout its lifecycle when the office funds and manages OT and national security. The plan must, at a minimum:

(a) Grant programs the authority to manage OT per program office leadership guidance;

(b) Define the scope of applicability of OT across the federal or site program;

(c) Demonstrate effective resource management by identifying performance metrics and objectives, including budget, timeline, and quality standards;

(d) Define a process for the sites to report to the Field Office OT that connects to an accreditation boundary; and

(e) Ensure OT complies with appropriate cybersecurity statutes and regulations.

(5) Implement processes and procedures for the federal and contractor acquisition, operation, maintenance, digital assurance, and disposition of OT and NSS under their cognizance as needed to implement their programs.

h. Critical Decision (CD) Gate Approval Authority.

(1) Approves all program or project CD gates for an assigned IT investment not to exceed $25 million (M), or as authorized by NA-IM.

(2) Approves new requirements that were not included in the annual supporting documentation for IT Investment budget submissions, not to exceed $25M, unless authorized by NA-IM.

i. Field Office Manager.

(1) Reviews M&O IT purchases that meet or exceed the thresholds established in Attachment 2.

(2) Supports and implements IT procurements and acquisitions, investment reviews, sound resource management, program governance and oversight, portfolio management, workforce strategies, and reporting requirements.

(3) Submits procurements and acquisitions for IT or IT services to NA-IM for review as well as requests for IoT device waivers when IoT devices do not comply with *IoT Cybersecurity Improvement Act of 2020* standards and guidelines.

(4) Coordinates with NA-IM regarding oversight and review of the M&O-managed IT.

(5) Delegates responsibilities to equivalent federal personnel as needed.

j. Senior Acquisition Official or Equivalent. Reviews and validates IT procurements that meet or exceed the monetary thresholds established in Attachment 2.

k. Information Technology Program/Project Manager.

(1) Supports the development and refinement of IT performance metrics, strategies, and other initiatives to support OMB's IT portfolio management reporting including data published on the Federal IT Dashboard in coordination with NA-IM.

(2) Ensures IT investments are included in budget requests and includes appropriate program management and project management items necessary to properly manage IT investments.

(3) Approves minor changes to planned IT procurements as long as the planned IT procurement:

(a) Is not already approved (following the submission of supporting documentation and the bill of materials during the annual budget approval process); and

(b) Does not exceed $1M for an individual purchase and $25M in IT investment implementation costs.

(4) Reviews and approves new IT investment requirements before requesting their CD Gate Approval Authority's approval to optimize the service delivery of their IT investment.

(5) Reviews IT investments procured as part of a Strategic Partnership Project.

l. NNSA Employees. In addition to the responsibilities identified in DOE O 203.1, *Limited Personal Use of Government Office Equipment including Information Technology*, NNSA employees must:

(a) Use government furnished technology in an appropriate manner, and in accordance with related job requirements.

(b) Use personal devices (to include mobile devices) in a manner that protects DOE/NNSA data and does not compromise IT assets.

(c) Refrain from using any DOE/NNSA IT system or network to intentionally search, view, or receive digital content that:

(i) is sexually explicit, sexually oriented, or sexual in nature;

(ii) conducts or furthers any type of illicit or illegal activity.

(d) Reports improper or unsafe use of IT to their immediate manager.

m. Contracting Officers.

(1) Include the CRD in any contracts that involve the acquisition of, or modification to IT and information systems in conjunction with the program or field office.

(2) Ensure the Contractor Purchasing System Approval is updated to align with the requirements of this SD.

(3) Ensure, prior to award of a contract, order, or work assignment for IT products or services, that the site's procurement:

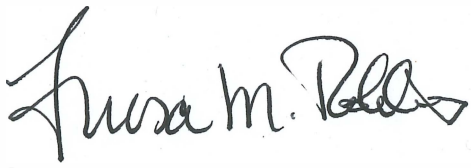
(a) Is associated with a previously approved IT investment; and

(b) Has received appropriate approvals in accordance with this Directive.

8. REFERENCES. See Attachment 5.

9. CONTACT. Office of the Associate Administrator for Information Management and Chief Information Officer, (202) 586-1729.

BY ORDER OF THE ADMINISTRATOR:



Teresa M. Robbins,
Acting Under Secretary for Nuclear Security
and Administrator, NNSA

Attachments:

Attachment 1: Contractor Requirements Document
Attachment 2: Investment and Procurement Approval Process
Attachment 3: Information Technology Portfolio Management Budget Process
Attachment 4: Definitions
Attachment 5: References

ATTACHMENT 1: CONTRACTOR REQUIREMENTS DOCUMENT NNSA SD 200.1A, *INFORMATION RESOURCES MANAGEMENT*

This Contractor Requirements Document (CRD) establishes requirements for National Nuclear Security Administration (NNSA) contractors who manage, operate, and have access to NNSA and Department of Energy (DOE) information systems. Contractors must comply with the requirements listed in this CRD and all applicable Attachments.

Regardless of the performer of the work, contractors are responsible for complying with and incorporating the appropriate CRD requirements into subcontractor contracts at any tier, to the extent necessary, to ensure the contractors comply with the requirements. The contractors must ensure that they and their subcontractors incur only those costs that are reasonable and would be incurred by a prudent person in the conduct of a competitive business.

1. REQUIREMENTS. Contractors must:

   a. Ensure that the procurement, acquisition, and management of information, information systems, and information technology (IT) complies with all applicable laws, regulations, and policies, including Office of Management and Budget (OMB) directives and guidance, the *E-Government Act of 2002,* the *Federal Information Technology Acquisition Reform Act,* the *Clinger Cohen Act of 1996,* the *Federal Information Security Modernization Act of 2014*, the *IoT Cybersecurity Improvement Act of 2020,* and DOE Order (O) 200.1A, *Information Technology Management*.

   b. Ensure the procurement, acquisition, use, and management of IT funded by or operated for the U.S. Government meet U.S. Government program and mission goals to promote sound resource management.

   c. Itemize information collection and IT in all procurements to enable the Field Office Manager (FOM), the managing program office, and the Office of the Associate Administrator for Information Management and Chief Information Officer (NA-IM) to review, assess, and approve the procurement or acquisition in accordance with the established dollar thresholds in Attachment 2.

   d. Develop applicable mobile device management procedures in a manner that cost-effectively reduces risk to an acceptable level while supporting mission requirements. The procedures must ensure:

      (1) Employees are appropriately trained in the use of both government-furnished and personally owned mobile devices to access information resources;
      (2) Monitoring and reporting on the effectiveness of mobile device management procedures; and
      (3) Overall accountability for mobile device use is retained.

e. Develop guidance to support telework, implement new and emerging telework technologies for enterprise use, and protect IT government-furnished and personally owned equipment used to remotely access NNSA information systems during telework from malware, hacking, and other cybersecurity threats.

f. Develop an Internet Protocol Version 6 Implementation Plan and submit the plan to DOE in accordance with OMB Memorandum (M)-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*, and DOE Order 200.1A, *Information Technology Management*.

g. Establish a site governance board to approve IT investment proposals, ensure alignment with the NNSA Enterprise architecture, approve site IT budget expenditures, and perform IT oversight. The site governance board must approve and forward all investment proposals that meet or exceed the monetary thresholds established in Attachment 2 to the NNSA IT Investment Review Board following concurrent approvals from the Field Office Senior Acquisition Official (SAO) and FOM.

h. Develop a site-specific IT portfolio management plan consistent with the guidelines established in Attachment 2. The plan must be periodically reviewed and updated to incorporate objectives established in the NNSA IT and Cyber Program Evaluation Guidance and NNSA and site-specific information resources plans. The IT portfolio management plan must:

(1) Establish or identify an IT Governance Board.
(2) Establish roles, responsibilities, and procedures for appropriate review and approval of IT acquisitions and procurements in accordance with the process outlined in Attachment 2.
(3) Require reviews to evaluate information resources, as necessary, to ensure the objectives and implementation factors identified in the annual IT PEG are being met.
(4) Report all IT requirements in accordance with OMB Circular A-11, *Preparation, Submission and Execution of the Budget*, guidance.

i. Implement this CRD 180 days from publication for existing contracts, if it is prior to the next contract award, renewal, or extension. For all other contracts, requirements must be implemented in accordance with the timelines established in DOE Acquisition Regulation clause 970.5204-2, *Laws, regulations, and DOE directives*.

2. <u>RESPONSIBILITIES.</u>

a. <u>Contractors supplying information systems and IT, including IT services, to NNSA.</u>

Ensure the requirements of this CRD and Attachments 2-5 are followed.

b. Management and Operating (M&O) IT Investment Program/Project Managers.

(1) Approve minor changes to planned IT procurements as long as the planned IT procurement:

(a) Is not already approved (following the submission of supporting documentation and the bill of materials during the annual budget approval process); and

(b) Does not exceed $1 million (M) for an individual purchase, or $25M in annual IT investment implementation costs.

(2) Review and approve new IT investment requirements prior to requesting approval of the Critical Decision (CD) Gate Approval Authority.

(3) Review IT procured as part of a Strategic Partnership Project (deferring to the sponsor for federal decisions, as applicable).

c. M&O Chief Information Officers, Information Technology Points of Contact, or appointed delegates.

(1) Review and approve, per the Site IT Governance Board recommendations, all contracts or other agreements for information, information systems and IT, including services where the requestor is a M&O contractor, the request is less than or equal to $25M, or the request does not fit the definition of a Major IT Investment. The review and approval of the IT investment can be delegated or assigned to a Program Manager or CD Gate Approval Authority.

(2) Review their site's proposed IT acquisition or procurement requirements greater than $25M or that meet the definition of a Major IT Investment and forward to their Field Office SAO and FOM for approval.

(3) Facilitate the submission of IoT device waiver requests to NA-IM in coordination with the FOM. Ensure that procurements and acquisitions for IT or IT services are disclosed to the FOM for NA-IM review.

(4) Ensure data for all IT and operational technology (OT) acquisitions are made available to the FOM in accordance with the established dollar thresholds in Attachment 2. The IT acquisition, except for OT, must be associated with an IT investment Unique Investment Identifier (UII). All approvals under this section must be sent to NNSA-OCIO-FITARA@nnsa.doe.gov.

d. Site IT Governance Review Board, or Similar IT Governance Board.

(1) Reviews all proposed IT investments in contracts or other agreements that include the procurement of IT, including acquisition for information, information systems, and IT and services for investments that are less than the monetary thresholds established in Attachment 2. When proposed investments meet or exceed the monetary thresholds established in Attachment 2, forward to NA-IM via the Field Office SAO and FOM.

(2) Ensures all information and IT procurements and acquisitions are reported to the NNSA FOM or designee prior to procurement or acquisition.

ATTACHMENT 2: INVESTMENT AND PROCUREMENT APPROVAL

Note: This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations. In addition to the requirements set forth in the Contractor Requirements Document (CRD), Attachment 1, contractors and subcontractors are responsible for complying with this Attachment and must incorporate it into contracts and subcontracts that include the CRD.

1. PURPOSE. Pursuant to the authority provided to the agency Chief Information Officer (CIO) and key bureau CIOs under the *Federal Information Technology Acquisition Reform Act* (FITARA), NNSA Delegation Order No. NA-005.01, Department of Energy (DOE) Order (O) 200.1A, Information Technology Management, and DOE O 415.1, Information Technology Project Management, this Attachment assigns information technology (IT) management responsibilities to NNSA Program Office Officials, Functional Office Officials, and management and operating (M&O) site Points of Contact, provided that the Officials confirm that all procurements are associated with an IT investment Unique Investment Identifier (UII) and are within the defined dollar thresholds. The Office of the Associate Administrator for Information Management and Chief Information Officer (NA-IM) may assign IT investment decisions to Program and Functional Offices for mission-specific IT that is not managed directly by an M&O.

2. APPLICABILITY.

   a. All IT acquisitions or procurements by program offices, functional offices, field offices, and M&O site elements (NNSA Elements), including National Security Systems (NSS), internet of things (IoT) devices, and information systems.

   b. All acquisitions of IT equipment by a contractor under an existing contract (e.g., other direct costs) where both:

      (1) The IT is used by the U.S. Government directly or used by a contractor under a contract with the U.S. Government that requires the use of the IT but does not include IT acquired by a contractor incidental to a federal contract; and

      (2) The equipment was not previously approved under this process.

   c. Operational Technology does not require IT portfolio management reporting and procurement approvals through IT Portfolio Management (ITPfM).

3. IT APPROVAL PROCESS.

   a. IT investment approval processes and procedures have been split into two parts:

      (1) Guidance for investments in IT; and

      (2) Guidance for the authorization to procure those resources.

b. NNSA Elements are expected to exercise their associated IT management responsibilities depending on the nature of the IT being procured and need to demonstrate that they can effectively manage an IT governance mechanism, in which case they may be granted governance privileges over their IT. NNSA Elements that do not establish their own IT Investment Review Board (IRB) or a similar IT governance board must forward new IT investment proposal requests to the NNSA IT IRB at NNSA-OCIO-FITARA@nnsa.doe.gov.

4. IT INVESTMENT APPROVAL DECISION PROCESS.

a. NNSA Elements must divide their IT approvals into two categories:

(1) Business Justification. This category evaluates whether the investments align with NNSA's strategy, goals, and objectives, and aligns with federal law and policy. It also evaluates the investment's potential return on investment.

(2) Technical Impact. This category evaluates whether the investment is technically feasible. It also evaluates the investment's potential impact on NNSA's existing technology infrastructure.

b. For each IT investment, NNSA Elements must assign an IT Investment Program Manager (PM) to execute the development, deployment, integration, and management of day-to-day operations. The NNSA Element CIO, or delegate, must oversee all stages of the IT investment including authorizing new procurements, and any changes to the scope, budget, and schedule, to ensure the IT investment stays within the approved cost and implementation timeframe. Table 1AT2 captures the applicable NNSA Management Framework to be used for the authorization of IT Investments.

c. IT investments that are being acquired or procured for integration into existing ITPfM investments must manage or transition their authorities according to the investment/project value thresholds in Table 1AT2.

Table 1AT2. Investment and Applicable Project Management Framework

Investment	Oversight Authority
Individual Purchase Costs ≤ $1 million (M)	Element IT IRB[1]
Implementation Costs ≤ $25M	Element IT IRB
Proposed Major IT Investment and/or Implementation Costs > $25M	NNSA IT IRB

[1] The program office or Site's IRB will assign a gate authority if a program office or Site IRB exists. Otherwise, the NNSA IT IRB will assign the gate authority.

5. IT INVESTMENT APPROVAL DECISION PROCESS.

a. New IT purchases that were not captured in the bill of materials (BOM) supporting annual budget planning must be approved by the NNSA Element's authority within their assigned limits, which allows the ITPfM Investment PMs to approve administrative and minor changes without additional approvals.

b. The IT Investment PM must evaluate purchases for organizational compliance and impact, including:

(1) Ensuring correct alignment with their ITPfM investment and budget.

(2) Evaluating for possible foreign ownership, control, or influence risk.

(3) Suitability within the IT operations environment and IT service management.

(4) Cybersecurity architecture and monitoring requirements.

(5) Records management and privacy.

(6) Compliance with other federal laws.

(7) Compatibility with enterprise license agreements.

6. IT PROCUREMENT PROCESS.

a. Procurement approval, required by FITARA as codified in 40 U.S.C. 11319 and implemented by NNSA's Office of Partnership and Acquisition Services, is principally performed by NA-IM as part of the annual budget approval process by evaluating an investment's supporting documentation (e.g., NA-IM FITARA request form, Summary, Statement of Work, Total Cost Estimate, Request of Quotation, FOM approval), proposed BOM, and details of anticipated modernization and enhancements.

b. For procurements not previously approved through the budget submission process, where supporting documentation stated above exceeds the authorization assignments of the NNSA Element's PM or appointed Approval Authority, and for procurements for a ITPfM Major Investment, requests must be sent to NA-IM for approval at NNSA-OCIO-FITARA@nnsa.doe.gov. Sufficient supporting documentation must be provided to help facilitate timely approval. Otherwise, a notice of procurement must be sent to the NNSA IT IRB at NNSA-OCIO-FITARA@nnsa.doe.gov.

7. PROVISIONS.

a. The installation of any hardware or software on DOE networks must not introduce additional cybersecurity risks and must be approved by the appropriate Authorizing Official before integration to the IT network.

b. The authorization assignment must not be used to purchase IT components integral or ancillary to any project, the entirety of which has not already been approved through existing approval processes (e.g., NNSA or Element IT IRB).

c. All IT procured must be associated with an IT investment UII. IT reporting must include this number to indicate the proper procurement to the CD Gate Approval Authority.

8. LIMITATIONS.

a. In exercising the authority delegated in the authorization assignment, a delegate is governed by the rules and regulations of the policies and procedures prescribed by the Secretary of Energy or their delegate(s) and the NNSA Administrator or their delegate(s).

b. Nothing in the authorization assignment precludes NA-IM from exercising the authority delegated by the Administrator.

ATTACHMENT 3: INFORMATION TECHNOLOGY PORTFOLIO MANAGEMENT BUDGET PROCESS

Note: This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations. In addition to the requirements set forth in the Contractor Requirements Document (CRD), Attachment 1, contractors and subcontractors are responsible for complying with this Attachment and must incorporate it into contracts and subcontracts that include the CRD.

1. INTRODUCTION.

The purpose of this Attachment is to describe NNSA's information technology (IT) investment reporting process to the Office of Management and Budget (OMB). OMB Circular A-11, *Preparation, Submission and Execution of the Budget*, requires IT investments to be reported annually to OMB and made public via the Federal IT Dashboard.

2. PROCESS.

a. IT resources currently associated with reported investments in the NNSA IT Portfolio will already have a unique investment identifier (UII) to complete the procurement request.

(1) The NNSA Information Technology Portfolio Management (ITPfM) team must work with the responsible Point(s) of Contact (POC) to ensure that the new funding amounts are updated in the past year, current year, and budget year (BY) investment ledger tables in the ITPfM tool.

(2) The ITPfM Team must work with the responsible POC to include updates regarding new projects, risks, metrics, and artifacts, as appropriate per OMB reporting requirements.

(3) IT resource requests originating from management and operating (M&O) sites must follow the M&O approval process. M&O Chief Information Officers' (CIO) indirect spending must already have associated UIIs and be reported in the ITPfM tool. IT spending outside of the M&O CIO's budget must be examined to determine whether it is being reported in other investments. M&O CIOs must work with the NNSA ITPfM Team and other NNSA program offices to update all investments at the M&O site.

b. IT resources for programs not in compliance with ITPfM reporting requirements will not have a UII to complete the procurement request. Note that reporting requirements only pertain to IT and not operational technology.

(1) The NNSA ITPfM team must work with the responsible POC(s) to initiate an IT investment that creates a UII.

(2) The NNSA ITPfM team must provide ITPfM training to the new POC(s).

(3) The responsible POC(s) must then complete the investment form prior to the next reporting deadline, as established by the OMB.

(a) Draft – late August

(b) Pre-decisional – September/October

(c) President's Budget/Passback (Final) – January/February

c. All completed investments must be added to the NNSA IT Investment Portfolio for the NNSA ITPfM team to perform updates, respond to data calls, conduct IT Dashboard assessments, and account for investments in the annual OMB submission.

d. The NNSA ITPfM team provides the IT Portfolio to NNSA's Management and Budget (NA-MB), from which NA-MB will verify the accuracy of the IT Portfolio to the IT portion of the approved budget request.

e. The NNSA ITPfM team collects BY IT Budget Requests and provides a high-level IT Portfolio report to the NNSA CIO for approval. Upon approval, the IT Portfolio is submitted to the Department of Energy (DOE) CIO for final review.

f. The NNSA IT Portfolio is submitted by the DOE ITPfM team to OMB as a part of the DOE IT Portfolio Submission Package.

g. NNSA must integrate government-wide cost structures, technologies, IT resources, and solutions into NNSA ITPfM investments according to the implementation requirements established by DOE's and OMB's Technology Business Management Taxonomy.

ATTACHMENT 4: DEFINITIONS

Note: This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations. The following definitions are relevant to this directive.

a. Critical Decision Gate Approval Authority. Review and approval authority for all program critical decision gates, including emergent and new requirements, for an assigned information technology (IT) investment not to exceed $25 million (M) or as authorized by the NNSA Office of the Associate Administrator for Information Management and Chief Information Officer (NA-IM).

b. Energy Systems Acquisition Advisory Board (ESAAB). Supports the Department of Energy's (DOE) and NNSA's strategic objective of achieving and maintaining excellence in project management. The ESAAB advises the Secretary of Energy, the Chief Executive for Project Management, and Departmental Project Management Executives on enterprise-wide project management policy and issues and assists the Chief Executive on critical decision milestones for Major System Projects and performance baseline deviation dispositions with a Total Project Cost of $750M or greater, DOE Order 413.3, *Program and Project Management for the Acquisition of Capital Assets,* current version.

c. Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, Committee on National Security Systems Instruction 4009, *National Information Assurance Glossary,* dated 4-26-2010, and National Institute of Standards and Technology Federal Information Processing Systems 199, *Standards for Security Categorization of Federal Information and Information Systems,* dated 2-10-2004.

d. Information and Communications Technology or Services. Any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display, Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, dated 5-15-2019.

e. Information Resources. Refers to information and related resources, such as personnel, equipment, funds, and information technology, 44 United States Code (U.S.C.) § 3502.

f. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, 44 U.S.C. § 3502.

g. Information Technology. With respect to an executive agency means (A) any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or

information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware, and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract, 40 U.S.C. §11101(6).

h. Internet of Things (IoT) Devices. Devices that (A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and (B) can function on their own and are not only able to function when acting as a component of another device, such as a processor, 15 U.S.C. 278g-3e.

i. IT Investment Review Board, or Similar Governance Board. The final decision-making body at a program office, functional office, or management and operating site element that is assigned responsibility to ensure investments and expenditures on IT and IT services align with the mission, vision, and needs of the organization by conducting investment and procurement decision making, ongoing oversight, and oversight of IT acquisition and procurement.

j. IT Investment Program Manager. An individual responsible for managing a portfolio or program comprised of one or more projects, systems, solutions, or services. Although the projects start and end, the program essentially continues indefinitely to support one or more key mission functions. Reviews and approves minor and administrative changes to planned IT procurements.

k. Major IT Investment. Per the DOE definition, a Major IT Investment:

a. Has a cumulative steady state or mixed lifecycle funding of $25 million or more across the past year, current year, and budget year;

b. Is an OMB-directed portfolio IT investment;

c. Is a Government-wide E-Government, or Line of Business investment where DOE is a Managing Partner;

d. Is a Multi-Agency Collaboration or Inter-Agency Shared Services investment where DOE is an Agency Lead; or

e. Requires special management attention because of its importance to the mission or function of the Agency.

l. National Security System. A telecommunications or information system operated by the Federal Government, where the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or, subject to 40 U.S.C. 11103(2), is critical to the direct fulfillment of military or intelligence missions.

m. Operational Technology. Hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the Enterprise, 15 U.S.C. 278g-3a (6).

n. Program Execution Guidance. Provides the Nuclear Security Enterprise (NSE) with the priorities of NA-IM. Outlines the goals, objectives, and implementation factors necessary to ensure an effective IT program.

o. Technology Business Management (TBM) Taxonomy. A commercial standard to describe cost sources, technologies, IT resources (towers), and solutions. The TBM taxonomy has been adopted as government-wide policy to describe technology in common terms. The current TBM taxonomy is available at www.tbmcouncil.org.

THIS PAGE INTENTIONALLY LEFT BLANK

ATTACHMENT 5: REFERENCES

Note: This Attachment applies to National Nuclear Security Administration (NNSA) federal and contractor organizations. The following list contains references that are relevant to this directive.

a. *Clinger-Cohen Act of 1996*, as amended at 40 United States Code (U.S.C.) 11101, et seq.

b. *E-Government Act of 2002*, as amended at 44 U.S.C 3501, et seq.

c. *Federal Information Security Modernization Act of 2014*, as amended at 44 U.S.C. 3551, et seq.

d. *Federal Information Technology Acquisition Reform Act*, as amended at 40 U.S.C. 11302, 11319.

e. *FITARA Enhancement of 2017*, as amended at 40 U.S.C. 11302, 11319.

f. *GPRA Modernization Act of 2010*, as amended at 31 U.S.C. 1115.

g. *Government Performance and Results Act of 1993*, as amended at 31 U.S.C. 1115.

h. *Internet of Things Cybersecurity Improvement Act of 2020*, as amended at 15 U.S.C. 278g-3e.

i. Office of Management and Budget (OMB) Memorandum (M) 21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*.

j. OMB M-16-15, *Federal Cybersecurity Workforce Strategy*.

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

l. Office of Personnel Management guide, *Compensation Flexibilities to Recruit and Retain Cybersecurity Professionals*.

m. National Institute of Standards and Technology (NIST) Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity*.

n. NIST Federal Information Processing Systems 199, *Standards for Security Categorization of Federal Information and Information Systems*.

o. Department of Energy (DOE) Acquisition Regulation clause 952.204-77, *Computer Security*.

p. DOE Acquisition Regulation clause 970.5204-2, *Laws, regulations, and DOE directives*.

q. DOE Order (O) 415.1B, *Information Technology Project Management*.

r. DOE O 413.3, *Program and Project Management for the Acquisition of Capital Assets*, current version.

s. DOE O 203.1, *Limited Personal Use of Government Office Equipment Including Information Technology*, current version.

t. DOE O 203.2, *Mobile Technology Management*, current version.

u. DOE O 200.1, *Information Technology Management*, current version.

v. NNSA Delegation Order No. NA-2019-NA005.01, effective 2-11-2019.

w. NNSA SD 205.1, *Baseline Cybersecurity Program*, current version.