

Approved: 12-23-2008
Chg 1 (MinChg): 1-13-2017
Chg 2 (LtdChg): 8-11-2023

SUBJECT: INFORMATION TECHNOLOGY MANAGEMENT

1. **OBJECTIVES.** The Department of Energy’s (DOE) overarching mission, to advance the national, economic, and energy security of the United States and to promote scientific and technological innovation, is enabled, advanced, and reliant on information and information systems that must be effectively managed to ensure mission success.

This Order supports, and is consistent with, DOE P 413.1, *Program and Project Management Policy for the Planning, Programming, Budgeting, and Acquisition of Capital Assets*, current version; supports the statutory and regulatory requirements provided in the *Federal Information Technology Acquisition Reform Act* (FITARA); the Clinger-Cohen Act; the E-Government Act; the Government Performance Results Act; the Government Paperwork Elimination Act; and Departmental Directives that address effective information technology management of Federal information and information systems, and delineate Departmental requirements and responsibilities to address the following information technology (IT) management areas:

- a. **Acquisition, Use, and Management of IT.**
- (1) **Information Technology Strategic Planning.** Conduct strategic planning activities, consistent with performance-based and results-based management and in accordance with the Clinger-Cohen Act Sections 5113 and 5123, and FITARA.
 - (2) **Capital Planning and Investment Control.** Develop, implement, and maintain a Capital Planning and Investment Control process in compliance with DOE P 413.1, current version; Office of Management and Budget (OMB) Circular A-11; OMB Circular A-130, Management of Federal Information Resources, Parts 8 and 9; and Clinger-Cohen Act Sections 5112 and 5122, and FITARA.
 - (3) **Enterprise Architecture.** Maintain an Enterprise Architecture for the life-cycle management of information, information resources, and related IT investments in compliance with OMB Circular A-11; OMB Circular A-130 Parts 8 and 9, and FITARA; specifically to:
 - (a) Maximize DOE investment in information technology; and
 - (b) Ensure that information technology is aligned with DOE strategic goals.

- (4) Hardware and Software Acquisition. Ensure that DOE's acquisition, use, and management of IT hardware and software meet program and mission goals as well as promote sound resource management and a more cost-effective government, in accordance with Federal Acquisition Regulation Part 39, *Acquisition of Information Technology*; FITARA, and DOE O 413.3, *Program and Project Management for the Acquisition of Capital Assets*, current version; specifically to:
- (a) Promote consolidation of software package acquisition, volume purchasing arrangements, enterprise wide agreements and best practices in software implementation, consistent with the SmartBuy program, identified in OMB Memo (M-03-14), *Reducing Cost and Improving Quality in Federal Purchases of Commercial Software*.
 - (b) Ensure that all Departmental software engineering utilizes a risk and lifecycle based Software Quality Assurance (SQA) program, in compliance with DOE O 414.1, *Quality Assurance*, current version.
 - (c) Manage in accordance with Federal Acquisition Regulation (FAR):
 - 1 Establish centralized authorities to coordinate hardware and software purchases,
 - 2 Deploy acquisition strategies for IT hardware and software, designed to take advantage of volume discount savings,
 - 3 Promote use of common hardware and software configurations, where appropriate, and
 - 4 Adopt standard replacement policies to make the best use of existing resources.
- (5) IT Operations and Use.
- (a) Access for People with Disabilities. Ensure that all Departmental technology is accessible to employees and members of the public with disabilities, in compliance with Section 508 of the Rehabilitation Act.
 - (b) Web Policy. Ensure that DOE websites comply with OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, OMB Circular A-130, and established Departmental Web procedures.
 - (c) Personal Use. Promote requirements and assign responsibilities for employees' limited personal use of Government resources,

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

- (d) Public Access. Promote public access to DOE information through the effective use of IT.
 - (e) Software Piracy. Adopt procedures to prevent illegal or inappropriate use of software licenses.
 - b. Cyber Security Management. Comply with established security requirements for the protection and control of information, information systems, and matter required to be classified or controlled by statutes, regulations, and DOE Directives, including DOE O 205.1, *Department of Energy Cybersecurity Program*, current version; and DOE P 470.1, *Safeguards and Security Program*, current version, consistent with the Federal Information Security Modernization Act of 2014 (FISMA).
 - c. Spectrum Management. Ensure that all use of radio frequency spectrum is in compliance with Title 47 Code of Federal Regulations (CFR), Part 300, Manual of Regulations and Procedures for Federal Radio Frequency Management, and other key publications that provide requirements, standards, and procedures.
 - d. Records Management. Ensure that a records management program is maintained, consistent with DOE O 243.1, *Records Management Program*, current version.
 - e. Internet Protocol Version 6 (IPv6) Compliance. Implement enterprise IPv6-based networking and Internet connectivity. IPv6 compliance will improve operational efficiency, provide the general public with continued access to citizen services, ensure the Federal government is capable of accessing IPv6-only services, and keep pace with and leverage this evolution in networking technology. This Order:
 - (1) Complies with Office of Management and Budget (OMB) Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*, dated November 19, 2020; and FAR Part 11.002 (g), dated September 28, 2010.
 - (2) Supports DOE mission objectives and provides DOE benefits and functionality to the public as DOE supports future Internet technology and services growth and innovation.
 - (3) Increases security above DOE's existing Internet Protocol (IP) infrastructure and connectivity, acknowledging that changes in architecture or practices may be required.
2. CANCELS/SUPERSEDES. DOE O 200.1A Chg 1 (MinChg), *Information Management Program*, dated 1-13-2017. Cancellation of a directive does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the directive.

Contractor Requirements Documents (CRDs) that have been incorporated into a contract remain in effect throughout the term of the contract unless and until the contract or regulatory commitment is modified to either eliminate requirements that are no longer applicable or substitute a new set of requirements.

3. DEPARTMENTAL APPLICABILITY.

- a. DOE Elements. Except for the exclusions in paragraph 3.c., this Order applies to all Departmental elements, including those created after the Order is issued.
- (1) The Administrator of the National Nuclear Security Administration (NNSA) must ensure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.
 - (2) The Administrator of the Energy Information Administration (EIA) will assure that EIA employees and contractors comply with their respective obligations under this Order. Nothing in this Order will be construed to interfere with the EIA Administrator's authority to establish EIA-specific policies consistent with Section 205(d) of the DOE Organization Act, Public Law 95-91, or the Administrator's obligation to ensure limitations on uses and disclosure of data as required by Title V (Confidential Information Protection and Statistical Efficiency Act) of the E-Government Act of 2002, Public Law 107-347, unless disapproved by the Secretary.
 - (3) The Director of the Office of Intelligence and Counterintelligence (IN) will assure that IN employees and contractors comply with their respective responsibilities under this Order. Nothing in this Order will be construed to interfere with Senior Intelligence Officer's authority to establish IN-specific policies consistent with Director of National Intelligence Directives and Orders and Executive Order (E.O.) 12333, unless disapproved by the Secretary.
 - (4) For IPv6 compliance, this Order applies to:
 - (a) All DOE information and information systems, including those used, managed, or operated by a contractor, another agency, or other organization on behalf of the Department.
 - (b) All DOE employees, contractors, and all other users of DOE information and information systems that support the operation and assets of DOE.
 - (c) All new acquisitions of information systems using IP by or on behalf of DOE, as well as decommissioning existing IPv4 systems.

Systems under development must meet DOE requirements in a manner commensurate with the sensitivity of the data they store and transmit, and the current life cycle phase.

- (d) The Administrator of Bonneville Power Administration will assure that its employees and contractors comply with this directive.

b. DOE Contractors.

- (1) Except for the exclusions in paragraph 3.c., the CRD (Attachment 1) sets forth requirements of this Order and must be included in all contracts for the management and/or operation of DOE owned or leased facilities, hereafter referred to as site/facility management contracts, and in all management, operation, and other contracts that require the acquisition, development, modification, or maintenance of computer software and/or IT hardware.
- (2) For IPv6 compliance, the CRD (Attachment 1) also sets forth requirements of this Order that will apply to Management and Operating (M&O) contracts and non-M&O Major Site/Facility contracts as determined by Heads of Departmental Elements (HDEs).
 - (a) The M&O and non-M&O Major Site/Facility contracts that must include the CRD are those at sites and facilities that collect, create, process, transmit, store, or disseminate data on Federal information systems for DOE or on behalf of DOE.
 - (b) The CRD forms the basis for equivalent requirements that may be included in contract clauses or other contract provisions applicable to non-M&O, Advisory, and Assistance contracts that collect, create, process, transmit, store, or disseminate data on Federal information systems.

c. Exemptions/Equivalencies for DOE O 200.1A. Equivalencies and exemptions to this Order are processed in accordance with DOE O 251.1, *Departmental Directives Program*, current version.

- (1) Exemption. The Naval Nuclear Propulsion Program is excluded from this Order; however, consistent with the responsibilities identified in Executive Order (E.O.) 12344, section 7, the Director of the Naval Nuclear Propulsion Program will ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Order for activities under the Deputy Administrator's cognizance.
- (2) Exemption. Bonneville Power Administration (BPA) is excluded from activities pursuant to objective herein referenced in paragraph 1.a.(2) and requirement herein referenced in paragraph 4.a.(2) related to capital

planning and investment control. In addition, BPA is excluded from any and all activities pursuant to objective herein referenced in paragraph 1.a.(4) and any and all hardware and software acquisition requirements herein referenced in paragraph 4.a.(4) related to Federal Acquisition Regulations (FAR).

(3) For IPv6 compliance:

- (a) Exemption. National Security Systems, as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, Guideline for Identifying an Information System as a National Security System.
- (b) Exceptions. In unique circumstances where requirements for IPv6-only operation may be delayed for some period or indefinitely, exceptions may be made. Exceptions to IPv6-only requirements or schedule should follow DE approval processes and will be submitted to the Office of the DOE Chief Information Officer for awareness, reporting, and adjudication as needed.

1 The following three categories are exceptions that may be documented using this process:

- a Break Mission Exceptions. Mission situations where current operations make it logistically impossible to implement IPv6-only operations.
- b Technically Incompatible Exceptions. Information systems that are not compatible with IPv6-only implementation due to the age and configuration of the system.
- c Increased Risk Exceptions. Situations in which implementing IPv6-only would significantly increase the risk to current architecture or systems. When these systems reach end-of-life, there will be a plan for future systems to be IPv6-only compliant.

2 Exclusions may be granted for certain types of highly-specialized equipment or systems that do not function as general-purpose IT systems and are not acquired under standard IT acquisition or “refresh” processes.

- 4. REQUIREMENTS. Information Technology will be managed consistent with all statutory, regulatory, OMB and Departmental requirements, including the E-Government Act, FISMA, FITARA, the Government Performance Results Act, the Government Paperwork Elimination Act, and the strategic and operational plans of the Department. Integrated IT management will be administered by the Office of the Chief Information

Officer (OCIO) and supported by various working groups fulfilling the following requirements.

a. Acquisition, Use, and Management of IT.

(1) Information Technology Strategic Planning.

- (a) Maintain the Information Resources Management (IRM) strategic plan that links IT planning and investment decisions to program mission and goals and establishes Department-wide IT performance goals, objectives, and measures.
- (b) Conduct IT performance management, including the development of performance measures that are quantitative and outcome-oriented.

(2) Capital Planning and Investment Control (CPIC).

- (a) Implement CPIC processes that effectively manage the selection, control, and evaluation of Departmental IT investments, ensuring prioritization and sound management, including fulfilling OMB reporting requirements for IT investments, as detailed in OMB Circular A-11.
- (b) Ensure that projects and programs are utilizing a systems development lifecycle methodology that effectively manages the development and maintenance of IT systems.

(3) Enterprise Architecture (EA). Oversee a Department-wide enterprise architecture (EA), which supports mission needs and provides business value through collaboration among Departmental elements, including:

- (a) Compliance with OMB direction and DOE Directives;
- (b) A governance process that promotes integrated business analysis in support of management decision-making;
- (c) Alignment with the Capital Planning and Investment Control process; and
- (d) Maintenance of a target enterprise architecture aligned with Departmental and Program Secretarial Office (PSO) strategic plans.

(4) Hardware and Software Acquisition.

- (a) Perform software asset management including the tracking, licensing, and utilization of DOE's software license inventory.

- (b) Develop and maintain procedures to prevent illegal or inappropriate use of software licenses.
 - (c) Ensure that DOE IT hardware acquisition and replacement practices are consistent with Departmental strategic and operational plans and all statutory, regulatory, administrative, and OMB requirements. They will consist of processes which support DOE in making better hardware decisions and enhancing hardware management.
 - (d) Oversee Software Quality Assurance programs to ensure that all software owned or maintained by DOE is subjected to formal quality assurance, pursuant to DOE O 414.1, current version.
 - (e) Attachment 2 sets forth the Department's IPv6 acquisition requirements, in alignment with the Federal Acquisition Regulation (FAR) Part 11.002 (g), dated September 28, 2010, and OMB M-21-07.
- (5) IT Operations and Use.
- (a) Ensure software acquisition requirements adhere to the 1998 Amendment to Section 508 of the Rehabilitation Act requirements to provide access for people with disabilities.
 - (b) Ensure that OMB and established DOE web policy and website requirements are met and all public websites are available to persons with limited English proficiency, per Executive Order 13166, *Improving Access to Services for People with Limited English Proficiency*, and corresponding Secretarial memorandum, *Access to Programs and Activities by Persons with Limited English Proficiency*, dated 4-11-06.
 - (c) Promote appropriate personal use of government equipment, consistent with Departmental requirements.
 - (d) Promote procedures to prevent illegal or inappropriate use of software licenses.
- b. Cyber Security Management. Oversee cyber security policies, procedures, and practices to ensure that they are consistent with OMB and established Departmental requirements.
- c. Spectrum Management. Manage spectrum management processes consistent with regulatory guidance, OMB requirements, and the strategic and operational plans of DOE.

- d. Records Management. Manage records management processes consistent with regulatory guidance, OMB requirements, and the strategic and operational plans of DOE.
- e. IPv6 Management. Attachment 2 sets forth the Department's IPv6 implementation requirements, in alignment with OMB M-21-07.

5. RESPONSIBILITIES.

a. Chief Information Officer.

(1) Acquisition, Use, and Management of IT.

(a) Information Technology Strategic Planning.

- 1 Develops and maintains the DOE Information Resources Management (IRM) Strategic Plan.
- 2 Provides advice and assistance to the Secretary, Deputy Secretary, and other senior management on Department-wide IT management.
- 3 Reviews the results of internal and external compliance assessments and provides Department-wide direction or guidance, as appropriate.

(b) Budget, Planning, and Portfolio Management.

- 1 Reviews and approves Departmental IT budget requests.
- 2 Program offices will provide their IT budget requests to the CIO for review and comment (see 40 U.S.C. § 11315 (c)(2)). Program offices will address CIO comments and, to the extent possible, resolve differences with the appropriate Under Secretary before submission of the program office budget to the CFO by the established deadline. With the submission of its budget request to the CFO, each program office, other than NNSA, will confirm that its IT budget request has been reviewed and approved by the CIO.
- 3 For NNSA, following the Under Secretary's submission of the NNSA IT/cyber budget to the CFO, the CIO will have an opportunity to review the NNSA budget. The CIO will coordinate any differences initially with the CFO and NNSA Under Secretary, and any unresolved issues will be presented to the Secretary and Deputy Secretary for final disposition.

4 Departmental elements will ensure that any proposed reprogramming of funds from IT projects are reviewed and approved by the CIO and CFO before the Department submits the reprogramming request. For NNSA, the CIO will have an opportunity to review IT reprogramming requests before the CFO reviews and submits for the Department (see DOE Order 130.1, *Budget Planning, Formulation, Execution and Departmental Performance Management*, current version).

(c) Capital Planning and Investment Control (CPIC). Provides oversight and manages the CPIC process, including establishing the CPIC process, policies, and responsibilities.

1 Ensures that IT is acquired and information resources are managed consistent with statutory, OMB and Departmental requirements and priorities;

2 Ensures the development, management, and use of an optimal IT portfolio that best supports programmatic needs, minimizes potential risk, and provides the greatest return on investment;

3 Ensures the integration and alignment of the CPIC process with EA, cyber security, budget formulation, investment assessment/prioritization, strategic portfolio review, and other management processes;

4 Provides a means for senior management to monitor investments, and respective milestones, toward measuring progress;

5 Refines the CPIC process to ensure that appropriate estimates of all IT resources are included in the Department's annual budget request and appropriate performance data are collected.

(d) Enterprise Architecture (EA). Establishes and oversees an EA program and procedures to support making optimal decisions and develop and maintain a sound and integrated IT investment portfolio aligned with DOE's mission and strategic business goals:

1 Defines and documents EA through a federated framework for developing, aligning, and implementing IT acquisition, development, and maintenance activities, working collaboratively with DOE program management;

- 2 Identifies opportunities for collaboration, acquisition, and reuse of hardware and software solutions; and
 - 3 Provides reports, analyses, and recommendations to facilitate the strategic planning efforts of DOE program Secretarial Offices.
- (e) Hardware and Software Acquisition.
 - 1 Establishes and maintains Department-wide direction and guidance for systems development lifecycle methodology and processes.
 - 2 Provides a framework for incorporating appropriate new technologies into DOE's IT environment, consistent with Departmental strategic and operational plans and all statutory, regulatory, administrative, and OMB requirements.
- (f) IT Operations and Use.
 - 1 Leads DOE E-Government efforts, in collaboration with DOE programs, to improve productivity and service to customers.
 - 2 Establishes DOE requirements and procedural guidance for establishing, operating, and maintaining DOE public websites.
 - 3 Supports and operates DOE's primary website, www.energy.gov, in collaboration with the Office of Public Affairs, which has responsibility for its content.
- (2) Cyber Security Management. Leads DOE's cyber security program, working with DOE Programs and supporting senior management.
- (3) Spectrum Management. Establishes Departmental Directives for the Radio Frequency Spectrum Management Program, including appointing a Department Spectrum Policy and Planning Director and overseeing DOE's compliance with P.L. 107-77 (Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act of 2002).
- (4) Records Management. Maintains the records management program for DOE.
- (5) IPv6 Compliance.

- (a) Carries out the responsibilities of the Federal Agency CIO as required by Federal law, regulation, and policy regarding IPv6 implementation.
 - (b) Works with the HDEs (or their designated representatives) to ensure that their Federal information system environments contain compliant components.
 - (c) Serves as the HDE for the purposes of Federal information systems described in this Order for IT services provided by OCIO to other DEs, Labs, Sites, and facilities. This authority may be further delegated.
 - (d) Works with other HDEs (or their designated representatives) to coordinate implementation of the IPv6 requirements.
 - (e) Collects, analyzes, and reports Department-wide progress data regarding IPv6 implementation.
 - (f) Consults with HDEs and Site/facility managers regarding any exception requests.
- b. Departmental Elements, including NNSA.
- (1) Obtain approval from the CIO prior to the appointment of any Federal employee with the duties of CIO.
 - (2) Involve the CIO in the development of Technical Qualifications for selection and position descriptions for staff with the duties of a CIO.
 - (3) Include the CIO or designee on selection panels.
 - (4) Obtain input from the CIO for the annual performance reviews of individuals that perform the duties of a CIO.
- c. Chief Human Capital Officer. Coordinates with the CIO to ensure that service centers are staffed with IT and cyber-knowledgeable human capital professionals.
- d. CIO, the Chief Acquisitions Officer, and NNSA CIO. Develop a comprehensive IT acquisitions review process in accordance with these basic contours:
- (1) In order to provide guidance and gain insight into the IT portions of major capital asset projects, the CIO is seated on the Energy System Acquisition Advisory Board (ESAAB) as a full member.
 - (2) Acquisitions not subject to review by the ESAAB will continue to follow their respective program office approval process, which will include the CIO or the CIO's designee as a full participant whenever executive-level

approval is required, followed by a review through the Information Management Governance Board (IMGB).

- (3) For headquarters-managed projects and program offices without an IT project approval process, or at the election of the CIO based on a risk assessment, an Investment Review Board (IRB), under the auspices of the IMGB, will be convened to provide formal review and approval of IT projects. With respect to NNSA projects, the CIO may solicit an advisory review from the IRB.

e. Chief Financial Officer.

- (1) In conjunction with the CIO, ensures that IT investments meet Government Performance and Results Act performance goals and comply with the Clinger-Cohen Act and FITARA through appropriate planning and budgeting of resources.
- (2) Supports the CIO in the effective financial and project management of IT assets.
- (3) Assists in the implementation of requirements, processes, and systems for IT budget administration and program justification.
- (4) In conjunction with the CIO, interfaces with the Office of Management and Budget and the Congressional Appropriations Committees in matters related to the Departmental IT budget.
- (5) In conjunction with the CIO, develops program performance measures and manages Departmental IT through the Department's performance tracking system.
- (6) In conjunction with the CIO, for appropriate IT business lines, budgets for and maintains the Department of Energy Working Capital Fund.
- (7) Reviews and makes recommendations regarding Mission Need Statements (Critical Decision-0) for proposed acquisition of new IT capital assets.
- (8) Collaborates with the CIO to ensure the incorporation of IT initiatives in the Department of Energy Strategic Plan.
- (9) In conjunction with the CIO, provides for and assures the financial integrity, formulation, execution, and analysis of the Department's IT budget.
- (10) Establishes the process for the CIO to review and approve Departmental IT budget requests, and incorporates the process into the Internal Review Budget process.

(11) In conjunction with the CIO, works with program offices to identify appropriate investments for reporting as major IT business cases.

f. DOE Under Secretaries, including the NNSA Administrator.

(1) Acquisition, Use, and Management of IT.

(a) Information Technology Strategic Planning.

- 1 Ensure that programs under their authority have implemented this Order.
- 2 Direct respective contracting officers to reassess their project portfolios so as ensure that the requirements of this order are implemented and ensure that procurement requests for contracts include appropriate references to this Order and CRD requirements, if necessary.
- 3 Notify program managers of their responsibilities to define how changes in policy, technology, and workforce will impact their organizations, and implement information technology management requirements to achieve their mission segment architecture.
- 4 Support the OCIO in the development and implementation of Departmental IT Directives strategy, processes, and procedures.
- 5 Ensure senior-level Program Secretarial Office representation to serve on, support, and fulfill the membership responsibilities of the IT Council, Architecture Review Board, and EA governance activities.
- 6 Develop and maintain a Strategic Plan, and corresponding EA, that delineates the strategic direction of Program Secretarial Office programs, projects and organizational IT portfolio.
- 7 Maintain and use the EA to support strategic planning, budget formulation and execution, capital planning, and hardware and software acquisitions.
- 8 Support Federal, and Departmental, IT and E-Government initiatives.
- 9 Add the CIO to Performance Evaluation and Measurement Plan and Annual Lab Planning or equivalent processes, as appropriate.

- (b) Capital Planning and Investment Control. Execute program and office specific processes that support the Department-wide capital planning process; specifically:
 - 1 Demonstrate effective control of the cost, scope, and schedule of investments and corresponding projects; and
 - 2 Prioritize investments, based upon performance and results.

- (c) Enterprise Architecture. Participate in the development of the DOE EA to support mission needs; provide opportunities for active involvement in continued improvement of the DOE EA; and provide IT business value through collaboration among all Departmental elements by:
 - 1 Participating in the governance process, specifically with EA governance bodies, including the Architecture Review Board and Enterprise Architecture Working Group.
 - 2 Collaborating with contractors to establish direction, issues, and information needs of Departmental EA.
 - 3 Coordinating efforts to integrate a Department-wide architecture, including the development of architectures specific to individual Departmental elements.
 - 4 Supporting the identification of opportunities for collaboration, acquisition, and reuse of hardware and software solutions.
 - 5 Providing EA content to the OCIO and Departmental elements using common definitions, to ensure the effective integration and alignment of EA across DOE.

- (d) Hardware and Software Acquisition.
 - 1 Implement Departmental Directives, procedures, and practices for systems development lifecycle management.
 - 2 Encourage centralized coordination of hardware and software purchases, at and above the site level, where possible, so as to take advantage of volume purchasing arrangements.
 - 3 Oversee development and implementation of SQA processes and procedures to ensure that SQA management compliance.

(e) IT Operation and Use.

- 1 Ensure that all information technology is accessible, in accordance with Section 508 of the Rehabilitation Act.
 - 2 Support the OCIO in establishing DOE direction for the development and implementation of public websites.
 - 3 Ensure that websites are consistent with Federal and DOE policy, as stated in OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, and OMB Circular A-130.
 - 4 Verify that each site/facility management contractor's DOE-approved property management system provides guidance and limitations on personal use of Government resources.
- (2) Cyber Security Management. Leads organizational cyber security programs, consistent with DOE O 205.1, current version.
 - (3) Spectrum Management. Manage spectrum management processes consistent with regulatory and statutory guidance and OMB requirements.
 - (4) Records Management. Manage and secure information, records, and IT in accordance with National Archives and Records Administration and DOE policy and procedures.

g. Heads of Departmental Elements (HDEs) (including NNSA).

- (1) Establish priorities for their Offices, Sites, and M&O facilities to implement this Order and associated Federal IPv6 directives, incorporating feasibility and technical/programmatic risk considerations, and implementation costs, to flow down the requirements and responsibilities of this Order to all subordinate organizational levels through appropriate Federal information system direction across the Federal and contractor environment.
- (2) Review and approve or disapprove IPv6-only exceptions for Federal information systems under their purview that cannot be made compliant within the schedule set by OMB. Ensure that approved exceptions are tracked and reported to the OCIO.
- (3) Use a risk-based and tailored approach to flow down the requirements and responsibilities of this Order to all subordinate organizational levels through appropriate Federal information system direction.

- (4) May delegate specific responsibilities within this Order to other officials within the DE as appropriate.
 - (5) Ensure a determination is made as to which M&O and non-M&O Major Site/Facility contracts must include the CRD and notify COs to incorporate the CRD. Also ensure a determination is made as to which non-M&O, Advisory, and Assistance contracts must include equivalent requirements to the CRD (in a contract clause or other contract provision, for example, in the Statement of Work (SOW)), and notifies COs to include the equivalent requirements in the contracts.
- h. Heads of Departmental Elements (other than Under Secretaries and the NNSA Administrator).
- (1) Acquisition, Use, and Management of IT.
 - (a) Information Technology Strategic Planning.
 - 1 Ensure that programs under their authority have implemented this Order.
 - 2 Direct respective contracting officers to reassess their project portfolios so as ensure that the requirements of this order are implemented and that procurement requests for contracts include appropriate references to this Order and CRD requirements, if necessary.
 - 3 Notify program managers of their responsibilities to define how changes in policy, technology, and workforce will impact their organizations, and implement information technology management requirements to achieve their mission segment architecture.
 - 4 Support the OCIO in the development and implementation of Departmental IT Directives strategy, processes, and procedures.
 - 5 Ensure senior-level representation to serve on, support, and fulfill the membership responsibilities of the IT Council, Architecture Review Board, and EA governance activities.
 - 6 Develop and maintain a Strategic Plan, and corresponding EA, that delineates the strategic direction of programs, projects and organizational IT portfolio.
 - 7 Maintain and use the EA to support strategic planning, budget formulation and execution, capital planning, and hardware and software acquisitions.

- 8 Support Federal, and Departmental, IT and E-Government initiatives.
 - 9 Add the CIO to Performance Evaluation and Measurement Plan and Annual Lab Planning or equivalent processes, as appropriate.
- (b) Capital Planning and Investment Control. Execute program and office specific processes that support the Department-wide capital planning process; specifically,
- 1 Demonstrate effective control of the cost, scope, and schedule of investments and corresponding projects; and
 - 2 Prioritize investments, based upon performance and results.
- (c) Enterprise Architecture. Participate in the development of the DOE EA to support mission needs; provide opportunities for active involvement in continued improvement of the DOE EA; and provide IT business value through collaboration among all Departmental elements by:
- 1 Participating in the governance process, specifically with EA governance bodies, including the Architecture Review Board and Enterprise Architecture Working Group.
 - 2 Collaborating with contractors to establish direction, issues, and information needs of Departmental EA.
 - 3 Coordinating efforts to integrate a Department-wide architecture, including the development of architectures specific to individual Departmental elements.
 - 4 Supporting the identification of opportunities for collaboration, acquisition, and reuse of hardware and software solutions.
 - 5 Providing EA content to the OCIO and Departmental elements using common definitions, to ensure the effective integration and alignment of EA across DOE.
- (d) Hardware and Software Acquisition.
- 1 Implement Departmental Directives, procedures, and practices for systems development lifecycle management.
 - 2 Encourage centralized coordination of hardware and software purchases, at and above the site level, where

possible, so as to take advantage of volume purchasing arrangements.

- 3 Oversee development and implementation of SQA processes and procedures to ensure SQA management compliance.

(e) IT Operation and Use.

- 1 Ensure that all information technology is accessible, in accordance with Section 508 of the Rehabilitation Act.
- 2 Support the OCIO in establishing DOE direction for the development and implementation of public websites,
- 3 Ensure that websites are consistent with Federal and DOE policy, as stated in OMB Memorandum M-05-04, Policies for Federal Agency Public Websites, and OMB Circular A-130.
- 4 Verify that each site/facility management contractor's DOE-approved property management system provides guidance and limitations on personal use of Government resources.

- (2) Cyber Security Management. Lead organizational cyber security programs, consistent with DOE O 205.1, current version.
- (3) Spectrum Management. Manage spectrum management processes consistent with regulatory and statutory guidance and OMB requirements.
- (4) Records Management. Manage and secure information, records, and IT in accordance with National Archives and Records Administration and DOE policy and procedures.

- i. DE and Federal Site CIOs. Provide direction on and coordinate IPv6 planning, implementation, and status/progress reporting for their DEs, Labs, Sites, and facilities.
- j. Contracting Officers. Once notified of contract applicability, incorporate the CRD into M&O contracts, and the CRD or equivalent requirements into non-M&O Major Site and facility contracts, and Advisory and Assistance contracts. The Statement of Work may include these requirements or the Order may be incorporated by reference into the contract.
- k. Governance Bodies. IT Boards and Councils established by senior officials will provide forums for discussion and coordination of progress and issues in Department-wide implementations. Governance boards will periodically review

the exceptions approved by HDEs for awareness, enterprise-level coordination, and consultation.

(1) Information Management Governance Board (IMGB).

(a) Acquisition, Use, and Management of IT.

1 Information Technology Strategic Planning.

- a Supports the integration of strategic planning with performance indicators, organizational structures, business processes, E-Government, human capital, security, information management programs, budget and capital planning and investment control, IT security management, and EA management in support of DOE mission efficiency and effectiveness.
- b Assists in developing Directives, resolutions, policies, plans, and procedures regarding information management.
- c Provides a forum for the dissemination of lessons learned and best practices on IT-related matters, issues, and technologies.

2 Hardware and Software Acquisition. Promotes collaboration and effective and efficient acquisition and use of information resources to reduce operational costs and improve the management and execution of IT investments in support of DOE missions.

3 Capital Planning. Maintains oversight of DOE's Capital Planning and Investment Control process by:

- a Facilitating the development, maintenance, and implementation of processes that maximize the value of IT acquisitions while assessing and managing the potential risks, in accordance with the Clinger-Cohen Act of 1996 and OMB guidance.
- b Ensuring full compliance with the E-Government Act of 2002.

4 Enterprise Architecture. Maintains oversight of the DOE EA by:

- a Facilitating the development, maintenance, and implementation of a sound and integrated

Department-wide EA, in accordance with the Clinger-Cohen Act of 1996, the Federal Information Security Management Act, and OMB guidance.

b Assisting in the development of strategic goals and objectives to drive, as appropriate, EA development toward Federal agency-wide initiatives that optimize DOE and Government IT operations and cost.

c Identifying opportunities for improving the integration of EA and CPIC processes to mature and enhance processes.

(2) Architecture Review Board (ARB).

(a) Oversees the EA program and approves the EA.

(b) Provides recommendations to the OCIO regarding strategies, approaches, products, costs, benefits, cost-benefit feasibility, risks of alternative investment options, and architectural alignment of enterprise and application architecture projects.

(c) Develops recommendations on priorities, common solutions, Directives, policies, plans, procedures, and changes to information management architectures.

(d) Maintains oversight of DOE EA by:

1 Managing the Departmental Transition and Sequencing Plan, which describes the key planning and implementation activities that support transitioning from the current business environment to the target business environment outlined in the Strategic Plan;

2 Facilitating communication with all Departmental elements regarding the EA and Program and Staff office architectures;

3 Reviewing and approving architecture-based recommendations and guidance proposed by the DOE Chief Enterprise Architect for submission to the IT Council;

4 Reviewing and approving Enterprise Architecture Working Group (EAWG) work products;

5 Developing and maintaining EA elements and work products, including enterprise reporting.

- (3) Enterprise Architecture Working Group (EAWG).
 - (a) Functions as the primary governing body for EA initiatives.
 - (b) Collaborates to integrate respective program and staff office architectures into the DOE EA.
 - (c) Performs activities related to the development, implementation, maintenance, and management of the EA.

- l. DOE Chief Enterprise Architect.
 - (1) Acts as the functional EA program manager, providing leadership and direction to groups supporting the EA effort (e.g., EAWG, ARB, Federal employees, contractors).
 - (2) Coordinates the development, management, and maintenance of the DOE EA.
 - (3) Submits appropriate EA work products to the ARB and IT Council for their review and approval.
 - (4) Provides subsequent EA guidance in conjunction with the ARB.

- m. Spectrum Coordination Group.
 - (1) Functions as the governing body for communications among DOE programs and DOE's Radio Frequency Spectrum Management Program.
 - (2) Provides the primary means for addressing radio frequency and spectrum management issues impacting multiple DOE organizational elements.
 - (3) Ensures that Department-wide approaches to radio frequency and spectrum management activities are developed and implemented in an integrated and consistent manner.

- n. Enterprise-Wide Agreement Integrated Project Team. Acquisition, Use, and Management of IT: Hardware and Software Acquisition.
 - (1) Functions as the primary governing body for enterprise-wide software initiatives.
 - (2) Supports efforts to maximize IT buying power, streamline the IT total acquisition lifecycle, and reduce total cost of ownership.
 - (3) Coordinates the development and implementation of Directives, policies and procedures supporting the identification, acquisition, oversight and compliance of enterprise-wide software.

- (4) Facilitates PSO enterprise-wide requirements inclusion into enterprise-wide agreements.
 - (5) Assesses candidate project alignment with the enterprise architecture.
 - (6) Identifies, communicates, and collects enterprise-wide opportunities and requirements of common IT assets across all program areas.
 - (7) Supports the Energy-Wide Strategic Sourcing Program, consistent with the SmartBUY program, to ensure improved efficiency and economies of scale in DOE's acquisition process.
- o. Chief Health, Safety, and Security Officer. Acting as DOE's central element responsible for safety aspects relative to public and worker health, and safety and environmental protection, provides advice and assistance to the Chief Information Officer concerning policy requirements and guidance necessary to implement this directive on software used for safety applications per requirements of DOE O 414.1, current version.
6. INVOKED STANDARDS. This Order does not invoke any DOE technical standards or industry standards as required methods. Any technical standard or industry standard that is mentioned in or referenced by this Order is not invoked by this Order. Note: DOE O 251.1, current version, provides a definition for "invoked technical standard."
 7. REFERENCES. See Appendix A.
 8. DEFINITIONS. See Appendix B.
 9. CONTACT. Questions concerning this Order should be directed to the Office of the Chief Information Officer, Deputy CIO for Enterprise Policy, Portfolio Management & Governance at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:



DAVID M. TURK
Deputy Secretary

ATTACHMENT 1
CONTRACTOR REQUIREMENTS DOCUMENT
DOE O 200.1A, INFORMATION TECHNOLOGY MANAGEMENT

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors whose contracts involve Information Resources acquired, created, or used under the scope of its contracts funded by or operated for DOE.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In addition to the requirements set forth in this CRD, contractors are responsible for complying with Attachment 2 to DOE O 200.1A, referenced in and made a part of this CRD, which provides program requirements and/or information applicable to contracts in which this CRD is inserted.

Program Secretarial Offices (PSOs) are responsible for the lifecycle management of all Information Resources acquired, created, or used under the scope of its contracts and must exercise appropriate stewardship of Information Resources consistent with contract performance objectives and in accordance with DOE efforts referenced herein. Therefore, contractors must manage Information Resources to support efficient and effective performance of their contract and mission objectives, and in accordance with DOE efforts regarding:

1. Acquisition, Use, and Management of IT.
 - a. Information Technology Strategic Planning. Maintain a strategic plan that coordinates IT planning and investment decisions and links contractor-specific missions and goals to the Departmental strategic plan, as well as:
 - (1) Implement an IT investment decision process that utilizes Enterprise Architecture principles.
 - (2) Implement and manage IT acquisition processes to achieve cost savings through appropriate IT hardware and software standards, negotiated buying arrangements, and refresh policies.
 - b. Capital Planning and Investment Control. Develop, implement, and maintain a Capital Planning and Investment Control (CPIC) process, as well as:
 - (3) Execute program and office specific processes that support Department-wide CPIC efforts by monitoring and demonstrating effective control of the cost, schedule, and performance of investments and corresponding projects.
 - (4) Implement appropriate internal policies regarding the acceptable use of IT assets.
 - (5) Prioritizing and selecting investments, based upon performance and results, as part of the budget development process.

- c. Enterprise Architecture. Maintain an Enterprise Architecture for the life-cycle management of information resources and related IT investments funded by or operated for DOE.
 - d. Hardware and Software Acquisition. Ensure the acquisition, use, and management of IT hardware and software funded by or operated for DOE meet program and mission goals to promote sound resource management, specifically to:
 - (1) Promote consolidation of software acquisition, volume purchasing arrangements, enterprise wide agreements and best practices in software implementation, consistent with the Program Evaluation Management Plan and/or the SmartBuy program.
 - (2) Implement a Software Quality Assurance (SQA) program that applies a graded, risk-based approach.
 - (3) Ensure compliance with negotiated contract procurement requirements for IT procurements:
 - (a) Deploy acquisition strategies for IT hardware designed to take advantage of volume discount savings.
 - (b) Promote use of common hardware and software configurations, where appropriate.
 - (c) Adopt standard replacement policies to make the best use of existing resources.
 - e. IT Operations and Use. Implement and manage IT operations and processes to ensure that information published to Federal service-to-citizens public websites are appropriate, timely, and accessible to the public and individuals with disabilities.
2. Internet Protocol Version 6 (IPv6) Compliance. Nothing in this CRD is intended to restrict the creation or dissemination of unclassified scientific research, in alignment with the scientific missions of the Department, National Security Decision Directive-189 (NSDD-189), the OPEN Government Act of 2007 (Public Law No: 110-175) and the OPEN Government Data Act (Title II of the Foundations for Evidence-Based Policymaking Act, Public Law 115-435).

This CRD is consistent with the federated nature of the DOE governance model and the roles and responsibilities as they relate to Management and Operating (M&O) Contract Partners (DOE P 112.1, *DOE Roles and Responsibilities – National Laboratories*, current version).

- a. The Contractor must institute an IPv6 program consistent with Departmental Element and Site Office federal direction to implement OMB Memorandum M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*, to

transition DOE information systems to operate solely using the IPv6 Internet addressing protocol. The contractor's IPv6 program must meet the requirements in Paragraph 2.b., below.

- b. Consistent with OMB M-21-07 and subsequent IPv6 guidance, all existing IPv4 equipment and systems will be upgraded to IPv6-only, and all new acquisitions of IP-enabled assets for Federal information systems will be IPv6 compliant to improve operational efficiency, provide the general public with continued access to citizen services, ensure the Federal government is capable of accessing IPv6-only services, and to keep pace with and leverage this evolution in networking technology.

(1) For IPv6 compliance:

- (a) Exemption. National Security Systems, as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, Guideline for Identifying an Information System as a National Security System, are exempted or excluded from implementation of this order.
- (b) Exceptions. In unique circumstances where requirements for IPv6-only operation may be delayed for some period or indefinitely, exceptions may be made. Exceptions to IPv6-only requirements or schedule should follow DE approval processes and will be submitted to the Office of the DOE CIO for awareness, reporting, and adjudication as needed.

1 The following three categories are exceptions that may be documented using this process:

- a Break Mission Exceptions. Mission situations where current operations make it logistically impossible to implement IPv6-only operations.
- b Technically Incompatible Exceptions. Information systems that are not compatible with IPv6-only implementation due to the age and configuration of the system.
- c Increased Risk Exceptions. Situations in which implementing IPv6-only would significantly increase the risk to current architecture or systems. When these systems reach end-of-life, there will be a plan for future systems to be IPv6-only compliant.

- (2) Implementation Plans. Detailed implementation plans for IPv6-only operation (and subsequent plan updates) must be submitted to the DEs for Labs, Sites, and facilities that acquire and operate Federal information

systems with IP-enabled assets. The plans must incorporate an intent to acquire IPv6-compatible equipment whenever it is available to meet requirements for specialized IT (e.g., scientific and operational-technology equipment and devices), and to transition general-purpose IT to IPv6 operation within the schedule established by OMB.

- (3) Acquisitions. For specialized IT, distinct from general-purpose commodity IT, the following acquisition requirements apply to the extent that IPv6-compliant equipment is available. Exceptions must be documented and justified in the procurement requests. For general-purpose IT and networking acquisitions, availability of IPv6-compliant acquisition options is assumed, and compliance is expected.
- (a) All hardware and system acquisitions, except for the exceptions noted above, made after inclusion of this clause into the pertinent contract, that are Internet Protocol (IP)-aware or perform IP functions, must be capable of operating in an IPv6-only mode.
 - (b) All software developed or acquired, except for the exceptions noted above, after inclusion of this clause into the pertinent contract, that incorporates direct IP-addressing or functionality, must also be capable of operating in an IPv6-only mode.
 - (c) Hardware and system acquisitions and software development, except for the exceptions noted above, should all meet the requirements of the U.S. Government v6 Profile (USGv6), defined in the most current version of NIST SP 500-267.

ATTACHMENT 2 INTERNET PROTOCOL VERSION 6 (IPv6) COMPLIANCE

This Attachment provides information and/or requirements associated with DOE O 200.1A as well as information and/or requirements applicable to contracts in which the associated CRD (Attachment 1 to DOE O 200.1A) is inserted.

Consistent with OMB M-21-07, all existing IPv4 equipment and systems will be upgraded to IPv6-only and all new acquisitions of IP-enabled assets for Federal information systems will be IPv6 compliant to improve operational efficiency, provide the general public with continued access to citizen services, ensure the Federal government is capable of accessing IPv6-only services, and to keep pace with and leverage this evolution in networking technology. The OMB memo applies agency-wide, as do its progressively increasing compliance targets listed below.

All DOE Elements, Labs, Sites, and facilities that operate Federal information systems with IP-enabled assets must comply with OMB M-21-07, and subsequent future guidance and directives, including milestone schedules and technical standards. Unless superseded by subsequent government-wide guidance, OCIO will be coordinating compliance with all targets.

1. Implementation Plans.

- a. The Department maintains a high-level enterprise-wide implementation plan for IPv6-only operation. The enterprise-wide implementation plan provides a framework for integrating the detailed implementation plans and prioritizations developed by DEs, Labs, Sites, and facilities.
- b. Detailed plans for IPv6-only operation (and subsequent plan updates) must be submitted to the OCIO by each DE. These plans are expected to address their respective organization's unique architecture, systems, and priorities. The plans should document how each organization will contribute substantially to the overall DOE compliance targets by setting notional compliance targets of 100% wherever possible. Plans must be updated at least annually until completion.

2. Reporting. The DOE OCIO will establish a periodic reporting process to collect progress and status information from all DEs, Labs, Sites, and facilities that are responsible for implementing this change in IP operations in their Federal information systems with IP-enabled assets.

3. Acquisitions.

- a. All hardware and system acquisitions, except for the exceptions noted below, made after the execution of this Order that are IP-aware or perform IP functions must be capable of operating in an IPv6-only mode.
- b. All software developed or acquired, except for the exceptions noted below, after the execution of this Order, that incorporates direct IP addressing or functionality, must also be capable of operating in an IPv6-only mode.

- c. Hardware and system acquisitions and software development, except for the exceptions noted below, should meet the requirements of the U.S. Government v6 Profile (USGv6), defined in the most current version of NIST SP 500-267. Exceptions must be documented and justified in the procurement requests.
 - d. COs may rely on the requiring activity's declaration on the acquisition plan to determine the applicability of IPv6 requirements to its acquisition. When the acquisition plan and the requirements documents provided by the requiring activity establish the applicability of IPv6 in accordance with FAR 11.002, the contracting officer must:
 - (1) Include a contract requirements statement in solicitations that include a reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267B, USGv6 Profile) and the corresponding declarations of conformance defined in the USGv6 Test Program for products and services that use the IP, including that the products provide full feature functionality in both dual stack (IPv4 and IPv6) and IPv6-only environments in compliance with the USGv6 Test Program, unless the CIO waives the requirement.
 - (2) Include instructions in solicitations that require offerors to notify the CO of any contract specifications that do not comply with providing full feature functionality for IPv6.
 - (3) Include the following for IPv6 compliance: As established in Section 3.c.(3) of this Order:
 - (a) Exemption. National Security Systems, as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59, Guideline for Identifying an Information System as a National Security System, are exempted or excluded from implementation of this order.
 - (b) Exceptions. In unique circumstances where requirements for IPv6-only operation may be delayed for some period or indefinitely, exceptions may be made. Exceptions to IPv6-only requirements or schedule should follow DE approval processes and will be submitted to the Office of the DOE CIO for awareness, reporting, and adjudication as needed.
- 1 The following three categories are exceptions that may be documented using this process:
- a Break Mission Exceptions. Mission situations where current operations make it logistically impossible to implement IPv6-only operations.

- b Technically Incompatible Exceptions. Information systems that are not compatible with IPv6-only implementation due to the age and configuration of the system.
 - c Increased Risk Exceptions. Situations in which implementing IPv6-only would significantly increase the risk to current architecture or systems. When these systems reach end-of-life, there will be a plan for future systems to be IPv6-only compliant.
- 4. Contract Incorporation. The HDE, or their designee, shall notify the Contracting Officer (CO), and other appropriate subject matter experts in the organization, that the directive applies to an existing contract or to a solicitation for a future contract. For existing contracts, the HDE shall designate appropriate representatives to work with the CO to develop an appropriately tailored set of standards, practices, and controls.
 - a. CRD(s) must be added to contracts to include reference to this Order and IPv6 requirements.
 - (1) For existing M&O contracts (which should already be subject to previous requirements for IPv6-compatible IT acquisitions), the CO must provide the contractor the opportunity to assess the effect of incorporating the CRD on contract cost, funding, schedule, and technical performance, and to provide input on the appropriately tailored set of requirements for the contract. All associated activities will be accomplished in a timely manner and, if applicable, in accordance with the timelines established in DOE Acquisition Regulation 970.5204-2. The CO will incorporate the CRD without alteration unless the directive permits alteration, and the appropriate process is followed.
 - (2) For existing non-M&O contracts that include acquisition or management of IP-enabled information systems or equipment, the CO must attempt to incorporate the CRD bilaterally. If attempts to negotiate the CRD into the contract bilaterally are not successful, the CO must consult with the Head of Contracting Activity, Headquarters program office, and General Counsel. For non-M&O Advisory and Assistance contracts, the contracts must include equivalent requirements to the CRD (in a contract clause or other contract provision, for example, in the SOW).
 - b. Contracts that do not use a CRD must be amended to include reference to this Order and IPv6 requirements when IT/Operational Technology (OT) Components are included.
 - c. Annual program M&O performance assessment plans and metrics must include IPv6 planning and progress as part of their Federal information systems operations evaluation.

5. References. The following references are specific to IPv6. See Appendix A for a complete list of references associated with this Order.
 - a. IPv6 FAR Requirements: Federal Register, Volume 74 Issue 236, dated December 10, 2009)
 - b. OMB memorandum, M-21-07, “Completing the Transition to Internet Protocol Version 6 (IPv6),” dated November 19, 2020
 - c. NIST Special Publication (NIST SP) 500-267, “A Profile for IPv6 in the U.S. Government – Version 1.0,” dated July 2008

APPENDIX A: REFERENCES

1. Public Law (P.L.) 93-579, The Privacy Act of 1974, 5 U. S. C., Section 552a, available at <http://uscode.house.gov/download/pls/05C5.txt>.
2. FITARA, Title VIII, Subtitle D of the National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291.
3. P.L. 95-91, as amended, Section 644 (42 U.S.C. 7101 note).
4. P.L. 99-508, Electronic Communications Privacy Act of 1986, 18 U.S.C. 2511.
5. P.L. 100-235, the Computer Security Act of 1987, establishes a computer standards program in the National Institute of Standards and Technology (NIST) to provide Government-wide security, including training of persons who manage, operate, and use Federal computer systems.
6. P.L. 106-246, Section 508 of the Rehabilitation Act, as amended by the Fiscal Year 2001 Appropriation for Military Construction, requires Federal agencies to make their information technology accessible to people with disabilities.
7. P.L. 106-554, Section 515, establishes the requirement for an Information Quality Program for information disseminated electronically to the public.
8. P.L. 107-347, E-Government Act of 2002, establishes a Federal Chief Information Officer within the Office of Management and Budget, and establishes a broad framework of measures that require using Internet-based functionality to enhance citizen access to Government information and services.
9. P.L. 107-347, the Federal Information Security Management Act of 2002 (as amended), 44 U.S.C., Chapter 35, *Title III Information Security* (as amended) state that a comprehensive framework will be provided for ensuring the effectiveness of controls over information resources that support Federal operations and assets and for effective Government-wide management and oversight of the related information security risks.
10. Title 5, Code of Federal Regulations (CFR), part 734, Political Activity of Federal Employees.
11. Title 5, CFR part 2635, Standards of Ethical Conduct for Employees of the Executive Branch.
12. Title 10, CFR part 1010.103, Reporting Wrongdoing.
13. Title 41, CFR part 102-193, sets forth policies and procedures concerning the creation, collection, use, documentation, dissemination, and disposition of records maintained by Federal agencies and the National Archives and Records Administration.

14. Title 5, United States Code (U.S.C.) 552, the Freedom of Information Act (Public Law 89-487), as amended, establishes the right of citizens to request information from Federal agencies and establishes a framework of procedures to implement this right.
15. 5 U.S.C. 552a, the Privacy Act of 1974, (Public Law 93-549), as amended, establishes requirements for the collection, maintenance, and dissemination of personal information by Federal agencies.
16. 17 U.S.C. 101-810, the Copyright Act of 1976 (Public Law 94-553), dated 10-19-76, as amended, which establishes the rights and protections surrounding intellectual property.
17. 29 U.S.C. 794d, as amended by the Workforce Investment Act of 1998 (P.L. 105-220), dated 8-7-1998, and <http://www.section508.gov>.
18. 31 U.S.C. 501 note, addresses shortcomings in financial systems, internal controls, and the use of Federal assets and aims at producing more reliable and useful financial information, in part through the designation of an agency chief financial officer.
19. 31 U.S.C. 1101 note establishes the need for Federal agencies to implement performance measurement programs for their activities, including information management, that use measurable objectives to show whether an agency is getting appropriate value for its investments.
20. 41 U.S.C. Chapter 4 which imposes the responsibility for developing, maintaining, and facilitating the implementation of a sound, integrated IT architecture on Agency chief information officers.
21. 44 U.S.C. Chapters 21, 29, 31, and 33, specify the functions and responsibilities for managing Federal records and the procedures that must be followed to obtain approval for their disposition.
22. 44 U.S.C. Chapter 35 sets forth policies and procedures for the coordination of Federal information policy.
23. 44 U.S.C. Chapter 35 establishes a broad mandate for Federal agencies to perform information activities in an efficient, effective, and economical manner, and specifically recognizes the General Services Administration's role in the acquisition and management of computing resources.
24. 44 U.S.C. Section 3504, which directs Federal agencies to provide for the option of the electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper, and for the use and acceptance of electronic signatures when practicable.
25. 47 U.S.C. Sections 151–614, the Communications Act of 1934 (Public Law 73-416), as amended, provides for the regulation of interstate and foreign communication by wire or

- radio. In particular, Section 305(a) establishes Presidential statutory authority to authorize operations of radio stations belonging to, or operated by, the Federal Government. Section 606 establishes the war emergency telecommunications powers of the President. Sections 901-928 establish the National Telecommunications and Information Administration (NTIA).
26. Executive Order (E.O.) 12046, Relating to the Transfer of Telecommunications Functions, dated 3-27-78 delegates the Presidential responsibilities for management of the electromagnetic spectrum to the Secretary of Commerce and provides for the continuation of the Interdepartment Radio Advisory Committee to assist the Secretary in this authority.
 27. E.O. 12344 and 50 U.S.C. 2406 (Public Law 106-65).
 28. E.O. 13011, Federal Information Technology, dated 7-16-96, which integrates provisions of the Clinger-Cohen Act of 1996, the Paperwork Reduction Act of 1995, and the Government Performance and Results Act of 1993.
 29. E.O. 13103, Computer Software Piracy, dated 9-30-98, which delegates agencies' authority to establish and adopt procedures to ensure the use of legally licensed software.
 30. E.O. 13166 and Secretary Bodman memo, Access to Programs and Activities by Persons with Limited English Proficiency, date 4-11- 2006.
 31. Office of Management and Budget (OMB) Circular A-11, Preparation, Submission, and Execution of the Budget provides guidance on preparing fiscal year budget submissions and includes instructions on budget execution.
 32. OMB Circular A-130, *Transmittal Memorandum #4, Management of Federal Information Resources*, dated 11-28-00, establishes federal policy for the management of federal information resources.
 33. OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated 9-30-03.
 34. OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, dated 8-23-04.
 35. OMB Memorandum M-05-04, *Policies for Federal Agency Public Websites*, dated 12-17-04, provides, for the Heads of Executive Departments and Agencies, federal policy guidance for the management of information on agencies' public websites.
 36. NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

37. NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.
38. DOE P 226.2, *Policy for Federal Oversight and Contractor Assurance Systems*, current version.
39. DOE P 450.4, *Integrated Safety Management Policy*, current version.
40. DOE P 470.1, *Safeguards and Security Program*, current version.
41. DOE O 203.1, *Limited Personal Use of Government Office Equipment Including Information Technology*, current version, which establishes requirements and assigns responsibilities for employees' limited personal use of Government resources (office equipment and other resources including information technology) within DOE, including NNSA.
42. DOE O 205.1, *Department of Energy Cybersecurity Management Program*, current version. The purpose of the program is to protect all DOE cyber information and information systems by implementing the requirements of applicable laws to maintain national security and to ensure that DOE business operations proceed without security events such as interruption or compromise.
43. DOE O 221.1, *Reporting Fraud, Waste and Abuse to the Office of the Inspector General*, current version.
44. DOE O 243.1, *Records Management Program*, current version.
45. DOE O 413.3, *Program and Project Management for the Acquisition of Capital Assets*, current version, provides direction to project management for the acquisition of capital assets within DOE, with the goal of delivering projects on schedule, within budget, and meeting mission performance, safeguards and security, environmental, safety, and health standards.
46. DOE O 414.1, *Quality Assurance*, current version.
47. DOE O 415.1, *Information Technology Project Management*, current version.
48. DOE O 470.6, *Technical Security Program*, current version.
49. DOE O 471.7, *Controlled Unclassified Information*, current version.
50. DOE O 475.2, *Identifying Classified Information*, current version.
51. DOE G 414.1-4, *Safety Software Guide for Use with 10 CFR 830, Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*, current version.

52. DOE priorities, inventories, and schedules are located on the DOE home page under Web Policies at <http://www.energy.gov/webpolicies.htm>; and additional information is available on Webcontent.gov at http://www.usa.gov/webcontent/reqs_bestpractices/laws_regs/priorities_reqs/process.shtml.
53. DOE domain policy is located on the DOE home page at http://cio.energy.gov/services/dns_policy.htm.
54. OCIO Memorandum for All Headquarters Elements, *Policies for Federal Public Websites*, issued 8-4-06, and OCIO Memorandum for All Program Secretarial Officers, *Compliance with the Office of Management and Budget (OMB) Policies for Federal Public Websites*, issued 10-27-05.
55. CIO TMR-22, Protection of Sensitive Unclassified Information Including Personally Identifiable Information, dated October 17, 2007, located at http://cio.energy.gov/documents/DOE_CIO_TMR-22_-_SUI_101607_Final.pdf.
56. Usability information is located at <http://www.usability.gov/> and <http://www.usa.gov/webcontent/usability.shtml>.
57. Integrated Contractor Purchasing Team (ITCPT), additional information can be found at <https://icpt.llnl.gov/index.html>.
58. Electronic Product Environmental Assessment Tool (EPEAT) criteria, additional information can be found at <http://epeat.net/>.

APPENDIX B: DEFINITIONS

1. Architecture Review Board (ARB). The principal body charged with coordinating, reviewing and evaluating the implementation of the DOE EA.
2. Business Owners. Departmental entities that have an interest in IT management to support business needs.
3. Capital Planning and Investment Control (CPIC). A systematic approach to managing the risk and returns of IT investments for a given mission.
4. Computer Software Piracy. The use and or distribution of copyrighted computer software in violation of the copyright laws or applicable license restrictions. Common forms include end user piracy, counterfeiting, and hard-disk loading. End-user piracy occurs when an individual or organization reproduces and/or uses unlicensed copies of software for its operations by making more copies of the software than it is licensed for. Counterfeiting is the illegal duplication or distribution of software. Hard-disk loading occurs when a computer hardware reseller loads unauthorized copies of software into the machines it sells.
5. Departmental Element. A Departmental element is defined as a first-tier organization at Headquarters and in the Field. First-tier at Headquarters is the Secretary, Deputy Secretary, Under Secretary, and Secretarial Officers (Assistant Secretaries and Staff Office Directors). First-tier in the Field is Managers of the eight Operations Offices, Managers of the three Field Offices, and the Administrators of the Power Marketing Administrations. Headquarters and field elements are described as follows: (1) Headquarters elements are DOE organizations located in the Washington Metropolitan Area; and (2) “field elements” is a general term for all DOE sites (excluding individual duty stations) located outside of the Washington, DC, Metropolitan Area.
6. Enterprise Architecture (EA). A business-driven plan that describes the current state, future vision, and transitional states of an operation. This is presented in terms of: strategy and performance; business; applications and services; technology; data; and security, all at the end of a two-to-five year planning horizon.
7. Enterprise Architecture Working Group (EAWG). The principal body for DOE and Program Secretarial Office Enterprise Architecture integration initiatives.
8. Electronic Government. Electronic systems and networks that provide the public with access to or interaction with Government entities, services, information, and products without preference in a manner that acknowledges constitutional intent for privacy, security, and, if warranted, anonymity.
9. Hardware. Physical computer and other equipment used to process, store, or transmit computer programs or data.
10. Information Resources. Includes personnel, equipment, funds, and information technology.

11. Information Resources Management. The oversight of the acquisition and use of information resources to accomplish agency missions and to improve agency performance.
12. Information System. A combination of information, computer, and telecommunications resources and other information technology and personnel resources that collects, records, processes, stores, communicates, retrieves, and displays information.
13. 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).
14. Information Management Governance Board. Designated members responsible for coordinating information technology management within DOE.
15. Mission Critical System. Any telecommunications or information system that:
 - a. is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996;
 - b. is protected at all times by procedures established for information;
 - c. has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy; or
 - d. processes any information of which the loss, misuse, disclosure, or unauthorized access to or modification would have a debilitating impact on DOE's mission.
16. National Security System. As defined by Clinger-Cohen, any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, the command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions, and excludes any system used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

17. Office of the Chief Information Officer (OCIO). Responsible to ensure that IT is acquired and information resources are managed consistent with statutory, regulatory, and Departmental requirements and priorities.
18. Operational Technology (OT). 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.
19. Project Planning. The planning of project technical and management activities that are documented in a project plan. The plan typically describes the work to be done, the resources required, the methods to be used, the procedures to be followed, the schedules to be met, and the way the project will be organized. It includes a list of deliverables, actions required, and other key events needed to accomplish the project.
20. Project Tracking and Oversight. The tracking and reviewing of accomplishments and results against documented estimates, commitments, and plans. Includes the adjusting of plans based on actual accomplishments and results.
21. Quality Assurance.
 - a. A planned and systematic pattern of all actions necessary to provide adequate confidence that the item or product conforms to established operational, functional, and technical requirements.
 - b. A set of activities designed to evaluate the process by which products are developed or manufactured.
22. Quality Control.
 - a. The process by which product correctness is determined and action is initiated when nonconformance is detected.
 - b. A line function; the work done within a process to ensure that the work product conforms to standards/requirements.
23. Records Management. The planning, controlling, directing, organizing, training, promoting, and other activities related to the creation, maintenance and use, and disposition of records to achieve adequate and proper documentation of Federal policies and transactions and effective and economical management of agency operations.
24. Requirements Management. In system/software system engineering, the process of controlling the identification, allocation, and flowdown of requirements from the system level to the module or part level, including interfaces, verification, modifications, and status monitoring.
25. Risk Management. An approach to problem analysis that is used to identify, analyze, prioritize, and control risks.

26. Software. All software or software customized for DOE use, proposed for use, under development, or being maintained and used, whether that software was developed in-house, licensed from a commercial vendor for customized use, obtained from another organization, or otherwise acquired. The type of software includes, but is not limited to:
 - a. administrative/business-oriented software,
 - b. scientific/engineering software,
 - c. manufacturing-oriented software, and
 - d. process control (e.g., programmable logic control instructions).
27. Software License. A contract between a copyright holder and the licensee; a legal contract between a software application author or publisher and the user. The license is somewhat similar to a rental agreement, but it relates to rights to use intangible intellectual property rights instead of tangible goods. Under a typical license, the user agrees to pay for the privilege of using the software and promises the software author or publisher to comply with all restrictions stated in the license agreement.
28. Spectrum Coordination Group. Primary facilitator of communications among DOE spectrum stakeholders and the Spectrum Management Program, as well as the primary means of addressing wireless and spectrum management issues impacting multiple organizational elements of DOE.