U.S. Department of Energy
Washington, DC

CHANGE CHART

DOE O 200.1A

Chg 2 (LtdChg): 8-11-2023

SUBJECT: LIMITED/ADMIN CHANGE TO DOE O 200.1A, *INFORMATION TECHNOLOGY MANAGEMENT*

EXPLANATION OF CHANGES. Internet Protocol Version 6 (IPv6) is the next generation protocol and capable of providing an almost unlimited number of available IP addresses. IPv4 has been in use since 1983 and the global demand for IP-enabled assets is outpacing capacity. The Office of Management and Budget (OMB) issued Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6), November 19, 2020, to address this issue by communicating requirements and setting forth guidelines for the Federal government to transition to an IPv6-only environment.

OMB M-21-07 requires DOE to issue an agency-wide IPv6 policy. DOE O 200.1A, *Information Technology Management*, was selected for the inclusion of this IPv6 policy. The Order will supersede current interim policy memorandum titled, Department of Energy Complete Transition to Internet Protocol Version 6 (IPv6) Interim Solution, issued May 28, 2021.

1.

2. LOCATIONS OF CHANGES: Changes made throughout the document can be noted at the beginning of the chart.

Page	Paragraph	Changed	To
1	1	Added "current version"	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;
1	1	…and delineates Departmental requirements and responsibilities to address the following information technology (IT) management areas:	…and delineate Departmental requirements and responsibilities to address the following information technology (IT) management areas:
1	1.a.(2)	Added "current version"	Develop, implement, and maintain a Capital Planning and Investment Control process in compliance with DOE P 413.1, current version;
1	1.a.(3).(a)	Added "and"	Maximize DOE investment in information technology; and

Page	Paragraph	Changed	To
2	1.a.(4)	Added "current version"	…and DOE O 413.3, *Program and Project Management for the Acquisition of Capital Assets*, current version
2	1.a.(4).(b)	Removed DOE N 203, Software Quality Assurance; added "current version" to DOE O 414.1	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
2	1.a.(4).(c)	Added "Manage" and abbreviation for FAR	Manage in accordance with Federal Acquisition Regulation (FAR):
2	1.a.(5).(c)	Added "current version" for DOE O 203.1	… with DOE O 203.1, *Limited Personal Use of Government Office Equipment Including Information Technology*, current version.
3	1.b.	…including DOE O 205.1A, *Cyber Security Management*, and DOE P 470.1, *Integrated Safegards and Security Management*, consistent with the Federal Information Security Management Act of 2002 (FISMA).	…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).
3	1.d	Added "current version" to DOE O 243.1	
3	1.e	Added paragraph.	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

Page	Paragraph	Changed	To
			(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.
3	2.	CANCELLATION	CANCELS/SUPERSEDES
3	2	DOE O 200.1, *Information Management Program*, dated 9-30-96, expired. Cancellation of an Order does not, by itself, modify or otherwise affect any contractual or regulatory obligation to comply with the Order. A contractor requirement document (CRD) that has been incorporated into or attached to a contract remains in effect until the contract is modified either to eliminate requirements that are no longer applicable or to substitute a new set of requirements.	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.
4	3.	APPLICABILITY	DEPARTMENTAL APPLICABILITY
4	3.a.	Deleted Text	"(Please refer to www.directives.doe.gov/pdf/reftools/org_list.pdf for the most current listing of Departmental Elements.)"

Page	Paragraph	Changed	To
4	3.a.(1)	…(NNSA) will assure that NNSA employees and contractors comply with their respective responsibilities under this Order. Nothing in this Order will be construed to interfere with…	…(NNSA) must ensure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with…
4	3.a.(4)	Added subparagraph:	(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.
5	3.b.(2).	Added subparagraph	(2). For IPv6 compliance, the CRD (attachment 1) also sets forth the 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

Page	Paragraph	Changed	To
			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.
5	3.c.	Exclusions	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.
5	3.c.(1)	Added text.	Exemption. The Naval Nuclear Propulsion Program is exempted…
6	3.c.(2)	Added text	Exemption. Bonneville Power Administration (BPA) is excluded…
6	3.c.(2)	Deleted Text	Removed "in accordance with Secretarial Delegation Order 00 033.00A, dated 9-27-02" from the end of the paragraph
6	3.c.(3)	Added subparagraph	(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

Page	Paragraph	Changed	To
			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.
8	4.a.(4)(d)	Oversee Software Quality Assurance programs to ensure that all software owned or maintained by DOE is subjected to formal quality assurance,	Oversee Software Quality Assurance programs to ensure that all software owned or maintained by DOE is subjected to formal quality assurance,

Page	Paragraph	Changed	To
		pursuant to DOE N 203.1 and DOE O 414.1C	pursuant to DOE O 414.1, current version.
8	4.a.(4)(e)	Added subparagraph	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.
9	4.e	Added subparagraph	IPv6 Management. Attachment 2 sets forth the Department's IPv6 implementation requirements, in alignment with OMB M-21-07.
10	5.a.(1).(b).4	…and submits for the Department (see DOE Order 135.).	…and submits for the Department (see DOE Order 130.1, *Budget Planning Formulation, Execution and Departmental Performance Management*, current version).
12	5.a.(5)	Added Subparagraph	(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 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 implantation of the IPv6 requirements. (e) Collects, analyzes, and reports Department-wide progress data regarding IPv6 implementation.

Page	Paragraph	Changed	To
			(f) Consults with HDEs and Site/facility managers regarding any exception requests.
15	5.f.(1)(b)1	Added "and"	Demonstrate effective control of the cost, scope, and schedule of investments and corresponding projects; and
16	5.f.(2)	…consistent with DOE O 205.1A	…consistent with DOE O 205.1, current version.
16	5.g	Added subparagraph	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

Page	Paragraph	Changed	To
			Order to other officials within the DE as appropriate.
			(5) Ensure a determination in 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.
19	5.h.(2)	…consistent with DOE O 205.1A	…consistent with DOE O 205.1, current version.
20	5.i	Added subparagraph	DE and Federal Site CIOs. Provide direction on and coordinate IPv6 planning, implementation, and status/progress reporting for their DEs, Labs, Sites, and facilities.
20	5.j	Contracting Officers. Once notified, incorporates the requirements of the CRD into affected contracts. The Statement of Work may include these requirements or the Order may be incorporated by reference into the contract.	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.
20	5.k	Added Subparagraph heading, incorporated former standalone subparagraphs underneath (IMGB, ARB, EAWG)	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

Page	Paragraph	Changed	To
			implementations. Governance boards will periodically review the exceptions approved by HDEs for awareness, enterprise-level coordination, and consultation.
23	5.o	…per requirements of DOE O 414.1C, *Quality Assurance*.	…per requirements of DOE O 414.1, current version.
23	6	Added paragraph	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 251.1D, Appendix J provides a definition for "invoked technical standard."
23	8	Added Paragraph	8. DEFINITIONS. See Appendix B.
23		Deleted Paragraph "NECESSITY FINDING STATEMENT"	
Att. 1, P. 1	Leading Text	Second paragraph, deleted text	Deleted: "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."
Att.1, P.1	Leading text	Third paragraph: Therefore, contractors shall manage…	Therefore, contractors must manage
Att.1, P.2	2	Added Paragraph	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

Page	Paragraph	Changed	To
			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

Page	Paragraph	Changed	To
			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 Ssystem, 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

Page	Paragraph	Changed	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. |

Page	Paragraph	Changed	To
			(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.
Att.2, P.1		Added Attachment	See Attachment 2
App.B, P.2	13	Information Technology. Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency. For purposes of the preceding sentence, equipment is used by an Executive agency whether the equipment is used directly or by a contractor under a contract with the Executive agency that requires the use of such equipment or requires the use to a significant extent of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services, and resources.	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

Page	Paragraph	Changed	To
			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).
App.B, P.3	18	Added definition	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.