OCIO-OET-21-0004

U.S. Department of Commerce

United States Department of Commerce
Internet Protocol Version 6 (IPv6) Policy

September 2021

Table of Contents

1. PURPOSE

The purpose of this policy is to transition all Department of Commerce (DOC) information systems and services to Internet Protocol Version 6 (IPv6) by the year 2025 as mandated in the Office of Management and Budget (OMB) memorandum, M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)," dated November 19, 2020. This is the first issuance of this policy.

2. SCOPE

This policy applies to all existing DOC information systems including those used, managed, or operated by a contractor, another agency, or other organization on behalf of the DOC. Systems under development must meet the Federal acquisition guidelines for IPv6 as do all new DOC acquisitions of Information Technology (IT) products or services using Internet Protocol (IP).

3. BACKGROUND

OMB Memorandum M-21-07, dated November 19, 2020, outlines the Federal government's strategic mandate to deliver its information services, operate its networks, and access the services of others using only IPv6. This memorandum gives Federal agencies specific requirements for completing the operational deployment of IPv6 across all Federal information systems and services. The memorandum helps agencies identify and overcome obstacles that keep them from migrating to IPv6-only network environments.

4. AUTHORITY

Applicable Executive Orders, National Policy, and Public Laws for this policy include the following:

- CIO Council, "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government," July 2012
- Enterprise IPv6 Deployment Guidelines at datatracker.ietf.org
- FAR Part 39 – Acquisition of Information Technology, https://www.acquisition.gov/sites/default/files/current/far/html/FARTOCP39.html
- FAR Part 11.002(g) – *Describing Agency Needs – Policy*
- FAR Part 39 – *Acquisition of Information Technology*
- FAR Part 11.002(g) – *Describing Agency Needs – Policy*
- Federal Acquisitions Regulations (FAR) Part 11.002(g)Federal Information Security Modernization Act of 2014 (FISMA 2014) Public Law 113-283
- IAB Statement on IPv6, The Internet Architecture Board, November 2016
- IPv6 Enterprise Network Scenarios at https://datatracker.ietf.org/doc/rfc4057/

- IPv6 FAR Requirements: Federal Register, Volume 74 Issue 236 (Thursday, December 10, 2009) (govinfo.gov)
- IPv6 Transition/Co-existence Security Considerations at https://datatracker.ietf.org/doc/rfc4942/
- OMB memorandum, M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)," dated November 19, 2020
- OMB Circular A-130, "Managing Information as a Strategic Resource"
- OMB Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005
- OMB, Memorandum for Chief Information Officers of Executive Departments and Agencies, Transition to IPv6, September 28, 2010
- OMB Circular A-130, "Managing Information as a Strategic Resource"
- Security Considerations at https://datatracker.ietf.org/doc/rfc4942/
- "USGv6 Profile," National Institute of Standards and Technology (NIST) Special Publication 500-267B Revision 1
- "USGv6 Test Program Guide," NIST Special Publication (NIST SP) - 500-281A, Revision 1, November 2020
- "USGv6 Suppliers Declaration of Conformity," NIST Special Publication (NIST SP), 500-281Ar1s, November 2020
- "USGv6 Capabilities Table," NIST Special Publication (NIST SP), 500-267Br1s, November 2020.
- "USGv6 Test Methods: General Description and Validation," NIST Special Publication (NIST SP), 500-281Br1, November 2020
- "Guidelines for the Secure Deployment of IPv6," NIST Special Publication (SP) 800-119, December 2010
- "Security and Privacy Controls for Information Systems and Organizations", NIST SP 800-53 Rev. 5
- DOC Transition to Internet Protocol Version 6 (IPv6), July 2021

5. POLICY

This policy implements OMB memorandum M-21-07 mandates for transitioning existing Federal networks, systems, and services to IPv6 and Federal Acquisitions Regulations (FAR) Part 11.002(g) requirements for the procurement of all new networked IT products or services. The DOC will phase out the use of IPv4 for all systems by the close of FY 2025. To accomplish this:

- All newly acquired networked Federal information systems shall be IPv6-enabled at the time of deployment to ensure the IPv6 only requirement is met no later than FY 2023.
- Opportunities for IPv6 pilots will be identified and at least one pilot of an IPv6-only operational system will be completed by the end of FY 2021. A report of the results will be provided to OMB upon request.
- An IPv6 implementation plan will be developed by the end of FY 2021 to update all networked Federal information systems (and the IP-enabled assets associated with these systems) to fully enable native IPv6 operation. The DOC Information Resources

Management (IRM) Strategic Plan will be updated as required. The IPv6 implementation plan shall describe the agency transition process and include the following milestones and actions:

  - At least 20% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2023.
  - At least 50% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2024.
  - At least 80% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2025.

- All Federal information systems that cannot be converted to use IPv6 will be identified, the finding justified, and a schedule provided for replacing or retiring these systems.
- All external partners will identify systems that interface with networked Federal information systems and develop plans to migrate all such network interfaces to the use of IPv6.
- The upgrade of public/external facing servers and services (e.g., web, email, Domain Name System (DNS), and Intrusion Prevention System (ISP) services), internal client applications that communicate with public Internet services, and supporting enterprise networks to operationally use native IPv6 will be completed as soon as practicable.

6. ADHERING TO FEDERAL IPv6 ACQUISITION POLICY REQUIREMENTS

DOC shall ensure that all future acquisitions of networked information technology include IPv6 requirements as mandated in FAR Council amendment issued in December 2009, unless the DOC CIO or designee waives the requirement. DOC, bureaus acquiring information technology using Internet Protocol shall develop requirements documents to include reference to the appropriate technical capabilities defined in the U.S. Government Version 6 (USGv6) Profile, National Institute of Standards and Technology (NIST Special Publication (SP) 500-267 and the corresponding declarations of conformance defined in the USGv6 Test Program. The DOC COP shall ensure that Federal IT systems are positioned to leverage the technical and economic benefits of IPv6, and eventually migrate to IPv6-only environments when appropriate.
In accordance with existing FAR requirements, DOC shall:

- Continue to use the USGv6 Profile to define agency or acquisition specific requirements for IPv6 capabilities when purchasing networked information technology and services, specifying the requirement for hardware and software to be capable of operating in an IPv6-only environment.
- Continue to require potential vendors to document compliance with such IPv6 requirement statements through the USGv6 Test Program; and
- In rare circumstances where requiring demonstrated IPv6 capabilities would pose undue burden on an acquisition action, provide a process for the DOC CIO to waive this requirement on a case-by-case basis. In such cases, the purchasing agency shall

request documentation from vendors detailing explicit plans (e.g., timelines) to incorporate IPv6 capabilities to their offerings.

A requestor in DOC bureau or office seeking to procure an IT product or service using IP must work with their Contracting Officer (CO) to ensure appropriate IPv6 requirements language is included in the following documents:

- Procurement Requests (PR),
- Advanced Procurement Plans (APP),
- Statements of Work (SOW),
- Requests for Proposal, and
- Awarded Contracts

7. EVOLVING THE USGv6 PROGRAM POLICY REQUIREMENTS

NIST will continue to update and expand the USGv6 Program and provide periodic updates to the USGv6 Profile to incorporate the latest Internet Engineering Task Force (IETF) specifications relevant to IPv6 technology. DOC shall continue to monitor updates from the USGv6 Program to ensure DOC and its constituent bureaus maintain consistency with IPv6 changes of other government agencies, as well as continue to monitor and adhere to updates from NIST as required per FISMA. DOC shall enforce the following policy requirements:

- Avoid any unnecessary duplication of generic testing requirements by leveraging the USGv6 Test Program for basic conformance and general interoperability testing of commercial products.
- Ensure that acquisition specific testing focuses on specific systems integration, performance, and information assurance testing not covered in the USGv6 Test Program.

8. ENSURING ADEQUATE SECURITY

To help ensure the security benefits of IPv6 for all Federal agencies, DOC shall ensure the following requirements are in place for all DOC's information systems:

- Include plans for full support of production IPv6 services in IT security plans, architectures, and acquisition.
- Validate all systems that support network operations or enterprise security services (e.g., identity and access management systems, firewalls and intrusion detection/protection systems, end-point security systems, security incident and event management systems, access control and policy enforcement systems, threat intelligence and reputation systems) are IPv6-capable and can operate in IPv6-only environments.
- Follow applicable Federal guidance and leverage industry best practices, as appropriate, for the secure deployment and operation of IPv6 networks.
- Ensure that all security and privacy policy assessment, authorization and monitoring processes fully address the production use of IPv6 in Federal information systems.

9. PRODUCT AND SERVICE PROCURES REQUESTS

The following are the requirements for DOC staff to follow to request procurement of IT products and services:

- Include appropriate IPv6 requirements language in PR and APP.
- Work with CO to ensure appropriate IPv6 requirements language is included in Statements of Work (SOW), RFPs and awarded contracts.
- Complete IPv6 IT Procurement Checklist and send to CO.
- Analyze the project requirements, the IPv6 requirements, and the product's capabilities as captured on the Supplier's Declaration of Conformity (SDoC) and submit analysis to CO.
- If procured via federal schedule, sole source, or credit card, then obtain SDoC from vendor and submit SDoC to CO.
- Notify CO of all contract specifications that do not comply with providing full feature functionality for IPv6.

10. CONTRACTING OFFICERS

The DOC Enterprise Services CO shall review APP to determine the applicability of IPv6 requirements to its acquisition. The CO shall ensure the APP and supporting documents are in accordance with FAR 11.002(g) IPv6 requirements by including:

- Instructions in solicitations that require offerors to notify the contracting officer of any contract specifications that do not comply with providing full feature functionality for IPv6.
- A Contract requirements statement in solicitations that specifically states that products and services that use Internet Protocol provide full feature functionality in IPv6-only environments in compliance with the NIST USGv6 Testing Program.
- The IPv6 requirements statement shall be substantially the same as the statement provided in FERC's contracting writing templates and the IPv6 IT Procurement Checklist.

11. VENDORS

Vendors shall complete and sign a Supplier's Declaration of Conformity (SDoC) that specifies and certifies the product's IPv6 capabilities to submit with the proposal.

12. POLICY COMPLIANCE

Only DOC's CIO or a designee may waive the IPv6 requirements and must do so in writing. A requestor within DOC or its constituent bureaus seeking a waiver to retain an IT product or service that does not meet the IPv6 compliance requirements specified in OMB-M-21-07, FAR 11.002(g), and in this policy must submit a signed request in memorandum format to the DOC'S CIO. All IT hardware, software and services that do not comply with Federal and DOC IPv6 requirements require written and signed approval from the CIO.

13. ROLES AND RESPONSIBILITIES

Roles	***Responsibilities***
Deputy Secretary (DepSec)	Ensures OMB IPv6 transition compliance and consistency across the agency; and Provides agency-wide guidance for IPv6 implementation.
Chief Information Officer (CIO)	Carries out the responsibilities of the Federal Agency CIO as required by Federal law, regulation, and policy; Leads and strategizes for cybersecurity infrastructure and operations; Designates the Chief Information Security Officer (CISO) to carry out the CIO's responsibilities for cybersecurity and IT account management; Designates the DCIO for Solutions & Service Delivery (OSCIO) to operate and maintain the information systems and infrastructure; Has the authority to set Agency-wide IT policy, including all areas of IT governance such as enterprise architecture and standards, IT capital planning and investment management, IT asset management, IT budgeting and acquisition, IT performance management, risk management, IT workforce management, IT security and

Roles	*Responsibilities*
	operations, and information security; and Approves or disapproves all IPv6 compliance waivers to this policy.
Chief Information Security Officer (CISO)	Carries out the Chief Information Officer security responsibilities under Federal Information Security Modernization Act of 2014 (FISMA) and serving as the primary liaison for the Chief Information Officer (CIO) to the organization's Information System Owners, and Information System Security Officers; Heads an office with the mission and resources to assist the organization in achieving more secure information and information systems in accordance with FISMA requirements; and Approves all IPv6 upgrades and new purchases.
Information System Owner (ISO)	Provides procurement, development, integration, modification, operation, maintenance, and disposal of an information system; Provides operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements); Provides the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls; Responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior); and

Roles	*Responsibilities*
	Reviews security assessment results from the Security Control Assessor.
Information System Security Officer (ISSO)	Maintains an inventory of all components of their information system; Monitors and checks for security alerts, advisories, and directives on an ongoing basis for all non-standard components of their information system; Ensures appropriate prioritization of remediation for non-standard IT resources; Responds to alerts, advisories, and directives related to components of the information systems by taking appropriate remediation actions within established time frames; Reports any issues associated with application of remediation actions; Assigns individuals to test remediation of information system components; Trains individuals assigned to test information system components as needed; Maintains distribution lists for alerts, advisories, and directives; Distributes alerts, advisories, and directives to information system users as appropriate or requested; Carefully considers the structure and content of error messages that are custom developed for an information system component; Configures the information system to prevent non-privileged users from circumventing malicious code protection capabilities; and Configures the information system to prevent non-privileged users from circumventing intrusion detection and prevention capabilities.

Roles	*Responsibilities*
DOC Cybersecurity and Risk Management Division (CSRM)	Assists information system owners and managers in carrying out their responsibilities; and Assists in verifying that remediation actions have been successful.

Effective Date:

Review Cycle: The review cycle for this policy is set at 3 years.

Approved By:

ANDRE MENDES

Digitally signed by ANDRE MENDES
Date: 2021.09.27 09:07:33 -05'00'

André V. Mendes
Chief Information Officer
U.S. Department of Commerce

–END–

APPENDIX A

ACRONYMS AND ABBREVIATIONS

Acronym	**Definition**
APP	Advanced Procurement Plans
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Contracting Officer
DCIO	Deputy Chief Information Officer
DOC	Department of Commerce
DNS	Domain Name Service
FAR	Federal Acquisition Regulations
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
IoT	Internet of Things
IRM	Information Resources Management
ISO	Information System Owner
ISP	Intrusion Prevention System
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OS	Office of the Secretary
PR	Procurement Requests
RFP	Requests for Proposal
SP	Special Publication
SOW	Statements of Work
SDoC	Supplies Declaration of Conformity
USG	U.S. Government
USGv6	U.S. Government v6 Profile

This page was last updated on August 30, 2021