National Archives and Records Administration

Transmittal Memo

DATE: May 17, 2021

TO: All Staff

SUBJECT: NARA 803, Internet Protocol Version 6 (IPv6) Policy

Purpose: This policy implements requirements established by Office of Management and Budget (OMB) Memorandum 21-07 (M-21-07), Completing the Transition to Internet Protocol Version 6 (IPv6).

Background/significant changes: All agencies must issue a policy implementing the Memorandum's requirements to phase out IPv4 information systems and to require that all new information systems are IPv6-enabled when deployed. This directive meets the policy requirement and sets out the IPv6 project team, stakeholders, milestones, and goals.

Available forms: None.

Cancelled forms: None.

Cancelled policy: None.

Related policy: None.

Effective date: This directive is effective date of signature.

Contact information: For questions regarding this directive, please contact Hung Nguyen, in the Office of the Chief Technology Officer, at 301-837-2006 or hung.nguyen@nara.gov.

Debra Steidel Wall

DEBRA STEIDEL WALL
Deputy Archivist of the United States

Attachment

National Archives and Records Administration

NARA 803
May 17, 2021

SUBJECT: NARA 803, Internet Protocol Version 6 (IPv6) Policy

803.1 Policy.

a. NARA’s strategic intent is to deliver its information services, operate its networks, and access the services of others using only Internet Protocol version 6 (IPv6). NARA will strategically phase out the use of Internet Protocol version 4 (IPv4) in NARA Information Technology (IT) systems, network equipment, and web tools. NARA will replace IPv4 with the next-generation protocol, IPv6. NARA must transition to IPv6 because:

(1) Internet protocol (IP) addresses are globally unique identifiers that distinguish one entity from another when communicating over the Internet. Each system or item that connects to the Internet can have a different IP number.

(2) IPv4 has a limited number of IP addresses. Since IPv4 was first created, the global demand for IP addresses has grown with the continually increasing number of users, devices, and virtual entities connecting to the Internet. As a result, IPv4 addresses are becoming scarce in all regions of the world.

(3) IPv6 exponentially increases the number of IP addresses available, compared to IPv4. Telecommunications carriers, internet service providers, and major websites are migrating to IPv6 and slowly discontinuing their use of IPv4. NARA must transition to IPv6 so we can continue to interact with other agencies, customers, and the public using the Internet.

b. We have established the following deadlines to migrate to IPv6:

(1) By September 30, 2021, we will complete at least one pilot of an IPv6-only operational IT system;

(2) By FY 2023, all new, networked IT systems will be IPv6-enabled when they deploy;

(3) By FY 2023, at least 20 percent of IP-enabled assets (IT systems, network equipment, and web tools) on NARANet will operate in an IPv6-only environment;

(4) By FY 2024, at least 50 percent of IP-enabled assets on NARANet will operate in an IPv6-only environment;

(5) By FY 2025, at least 80 percent of IP-enabled assets on NARANet will operate in an IPv6-only environment; and

(6) We will phase out the use of IPv4 for all current IT systems as soon as practical while meeting the above milestones.

c. Effective immediately, all acquisitions of networked IT systems, network equipment, and web tools must include IPv6 requirements.

(1) All acquisitions of networked information technology and services must specifically require that all hardware and software be capable of operating in an IPv6-only environment;

(2) All potential vendors for acquisitions of networked information technology and services must document their compliance with IPv6 requirement statements through the Department of Commerce, National Institute of Technology (NIST), USGv6 Test Program; and

(3) The Chief Information Officer may waive this requirement on a case-by-case basis, in rare circumstances, and where requiring demonstrated IPv6 capabilities would pose an undue burden on an acquisition action. Vendors seeking a waiver must provide explicit plans with deadlines for incorporating IPv6 capabilities into their offerings.

803.2 Scope and Applicability.

This policy covers acquisition, development, and use of all NARA IT systems, network equipment, and web tools that connect to the Internet. This policy does not cover national security systems.

803.3 Responsibilities.

In addition to the authorities delegated in NARA 101, NARA Organization and Delegation of Authority, the following responsibilities are assigned in order to effectively implement this policy:

a. **IPv6 Integrated Project Team (IPT) (Information Services (I), Strategy and Performance Division (MP), Office of General Counsel (NGC), Office of Innovation (V), and Office of the Chief Acquisition Officer (Z)):**

(1) Develops NARA's IPv6 implementation plan and identifies opportunities for IPv6 pilots on operational IT systems;

(2) Identifies and develops policies and processes necessary to support IPv6 migration and NARA's IPv6 implementation plan; and

(3) Periodically reviews agency progress against NARA's IPv6 implementation plan and recommends changes to policies, procedures, or migration goals, as needed.

b. **Chief Technology Officer:**

(1) Leads NARA's IPv6 Integrated Project Team (IPT);

(2) Works collaboratively with the IPv6 IPT to develop and maintain NARA's IPv6 implementation plan and identify suitable opportunities for IPv6 pilot projects;

(3) Ensures that NARA has appropriate governance structures in place to effectively govern and enforce NARA's IPv6 migration, modifies Systems Development Life Cycle processes and deliverables to incorporate IPv6 requirements for new and enhanced IT systems, and is accountable for the deadlines established for IPv6 migration; and

(4) Ensures the Information Resources Management (IRM) Strategic Plan includes NARA's IPv6 migration strategy.

c. **Deputy Chief Information Officer**:

(1) Ensures that IT security plans, architectures, and acquisitions include full support for production IPv6 services;

(2) Ensures that all IT systems and services specifically support all hardware and software operating in an IPv6-only environment;

(3) Ensures that all IT systems that support network operations or enterprise security services are IPv6-capable and can operate in IPv6-only environments;

(4) Follows applicable Federal guidance for securely deploying and operating IPv6 networks; and

(5) Ensures that all security assessment, authorization, and monitoring processes fully address the production use of IPv6 in NARA IT systems.

d. **Chief Acquisition Officer (Z)**:

(1) Ensures that all solicitations for networked information technology and services specifically require that all hardware and software be capable of operating in an IPv6-only environment; and

(2) Ensures that all potential vendors for acquisitions of networked information technology and services submit documentation of their compliance with IPv6 requirement statements through NIST's USGv6 Test Program or have a waiver from the CIO before being considered for contract award.

e. **Chief Information Officer (I)** may waive the requirement that a vendor document IPv6 compliance through NIST's USGv6 Test program. Such waivers will be granted infrequently, on a case-by-case basis, and only when the CIO has determined that requiring demonstrated IPv6 capabilities would pose an undue burden on an acquisition action.

803.4 Authorities.

OMB Memorandum 21-07 (M-21-07), Completing the Transition to Internet Protocol Version 6 (IPv6), November 19, 2020, and any successor memoranda: requires agencies to complete the transition to all-IPv6 systems and products by specific milestones, and to issue a policy effectuating these requirements.

NIST SP 500-267B, USGv6 Profile (Rev 1), November 2020, successor publications, and other NIST IPv6 standards publications: sets out the standards for IPv6 systems and products and a testing framework for potential vendors of networked information technology and services to document their compliance with IPv6 requirement statements.

CIO Council, Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government, July 2012: sets out guidelines for actions and changes needed to transition to IPv6 across Government agencies.

803.5 Public Release.

Unlimited. This directive is approved for public release.

803.6 Records Management.

Records created in accordance with this directive are primarily temporary records and covered by records series items in General Records Schedule (GRS) 3.1: General Technology Management Records, GRS 3.2: Information Systems Security Records, and GRS 6.3: Information Technology Records. Records retention periods are mandatory although they may be implemented via manual or automated means. Contact Corporate Records Management (CM) with any questions about managing and retaining these records.