CIO IL-21-01 Internet Protocol Version 6 (IPv6) Policy

Posted Date: 05/17/2021**Status:** Validated**Outdated on:** 05/17/2022

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO IL-21-01
May 17, 2021

GSA INSTRUCTIONAL LETTER

SUBJECT: Internet Protocol Version 6 (IPv6) Policy

1. Purpose. In accordance with Office of Management and Budget (OMB) Memorandum M-21-07 Completing the Transition to Internet Protocol Version 6 (IPv6), this Instructional Letter (IL) sets forth the General Services Administration's (GSA) enterprise-wide IPv6 policy, consistent with agency authorities and operational mission needs to complete the transition to IPv6, and retire IPv4. This IL incorporates applicable Federal policies, standards, and guidelines, including roles and responsibilities.

2. Background.

a. In August 2005, OMB issued M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6), requiring agencies to enable IPv6 on their backbone networks by June 30, 2008. In September 2010, OMB issued a memo entitled "Transition to IPv6," requiring Federal agencies to operationally deploy native IPv6 for public Internet servers and internal applications that communicate with public servers.

b. In November 2020, OMB issued Memorandum M-21-07 requiring agencies to complete the transition to IPv6, and to retire the use of IPv4. While OMB Memo M-21-07 rescinded both previous OMB memorandums, the following elements remain applicable:

(1) Upgrade public/external facing servers and services (e.g., web, email, DNS, ISP services, etc.) to operationally use native IPv6; and,

(2) Upgrade internal client applications that communicate with public Internet servers and support enterprise networks to operationally use native IPv6.

3. Applicability.

a. This IL applies to all GSA Federal employees, contractors, and vendors of GSA, who manage, maintain, operate, procure, or protect GSA systems and data, as well as all GSA Office of the Chief Information Officer (GSA IT) systems, and any GSA data contained on, or processed by, IT systems owned and operated by, or on behalf of, any GSA Service or Staff Office.

b. This IL applies to the Office of Inspector General (OIG) to the extent that the OIG determines it is consistent with the OIG’s independent authority under the IG Act, and it does not conflict with other OIG policies or the OIG mission.

c. This IL applies to the Civilian Board of Contract Appeals (CBCA) to the extent that the CBCA determines it is consistent with the CBCA's independent authority under the Contract Disputes Act and other authorities and it does not conflict with the CBCA's policies or the CBCA mission.

4. Policies and Procedures.

a. As required by M-21-07, this policy requires that, no later than Fiscal Year (FY) 2023, all new networked Federal information systems are fully enabled for native IPv6 operation at the time of deployment. To ensure secure and efficient operations, and to keep our transition progress in alignment with M-21-07, GSA will phase out the use of IPv4 for all systems consistent with established timeframes outlined in M-21-07 in FY23 through FY25. To that end GSA will:

(1) Ensure all existing networked Federal information systems are transitioned to IPv6-enabled; and

(2) Ensure all new networked Federal information systems are IPv6-enabled.

b. The National Institute of Standards and Technology's (NIST) United States Government IPv6 USGv6 Test Program will provide government-wide conformance and general interoperability testing of commercial product offerings. This program is coordinated, to the maximum extent possible, with existing industry driven test programs to minimize the burden on vendors. To avoid any unnecessary duplication of generic testing requirements. GSA will:

(1) Leverage the USGv6 Test Program for basic conformance and general interoperability testing of commercial products; and

(2) Ensure that agency or acquisition specific testing focuses on specific systems integration, performance and information assurance testing not covered in the USGv6 Test Program.

c. To ensure the secure deployment of IPv6, GSA will:

(1) Ensure that plans for full support for production IPv6 services are included in IT security plans, testing and change management activities, architectures, and acquisitions;

(2) Ensure that 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;

(3) Follow applicable Federal guidance and leverage industry best practices, as appropriate, for the secure deployment and operation of IPv6 networks; and

(4) Ensure that all security and privacy policy assessment, authorization and monitoring processes fully address the production use of IPv6 in Federal information systems.

5. Roles and Responsibilities. IPv6 roles and responsibilities are distributed as follows:

a. Office of the Chief Technology Officer (CTO). Manages GSA's IT Standards function. Responsibilities include reviewing and approving

requests for new software solutions (including IPv6 capabilities and parity with IPv4) to be added to the list of approved agency IT Standards.

b. Office of the Chief Information Security Officer (OCISO).

(1) Identifies, evaluates, and engineers GSA IT's security-related hardware and software (i.e., domain name system (DNS), firewalls, intrusion prevention);

(2) Conducts vulnerability and penetration testing (with parity between IPv4 and IPv6); and

(3) Reviews and recommends approvals (or rejections) of proposed security configurations in accordance with departmental and federal risk management standards.

c. Office of Digital Infrastructure Technologies (IDT).

(1) Customer Relationship Management Division (IDTR).

(a) Receives and processes incoming customer requests, responds to incidents and maintains configuration standards for IT end-user (e.g., laptop, mobile devices) solutions, which are supportive of approved configuration requirements for native IPv6, as appropriate; and

(b) Conducts Tier 1 and Tier 2 customer support and coordinates opening, resolving and closing IT service requests and incidents.

(2) Infrastructure Capabilities Division (IDTB).

(a) Identifies, evaluates, and engineers GSA IT's end-user (e.g., laptops, mobile devices) and infrastructure compute (e.g., physical and virtual servers) and network solutions (e.g., routers, switches, load balancers); and

(b) Coordinates closely with the Information Security Engineering (ISE) division to ensure IPv6 cybersecurity and operational capabilities are evaluated.

(3) Infrastructure Integration Division (IDTI). Designs, tests, and accepts/rejects proposed GSA IT's infrastructure compute, storage and network solutions, including ensuring the solution be an IPv6-only enabled asset, prior to its promotion in the production environment(s) within the timeframe requirements of the OMB memo and this policy.

(4) Infrastructure Management Division (IDTO).

(a) Operates and maintains GSA IT's infrastructure compute, storage and network solutions, including support of IPv6-only and (when authorized) dual-stack IPv4/IPv6 enabled assets, in pre-production and production environment(s); and

(b) Coordinates closely with the Information Security Operations (ISO) division to ensure cybersecurity and operational capabilities are maintained.

d. Business/System Owners. Understand the impact of migrating to an IPv6 only environment, including evaluating the potential impacts to budget and resources required to support completing the transition to an IPv6 only environment, and serve as liaison to the vendor community for supporting the agency's requirement for IPv6 readiness of cloud-based solutions (as originally required by OMB-2010).

e. Contracting Officers. Ensure that all new acquisition activities to award contracts and task orders associated with information technology include: (1) the addition of appropriate contract clauses; (2) the vendor(s) include the appropriate USGv6 conformance standards and attestation reports; and (3) that ongoing performance of the contract/task order is supportive of Federal and GSA requirements, playbooks and framework requirements for IPv6.

f. IPv6 Integrated Project Team (IPT) which was established to meet the requirements of OMB M-21-07; to serve as the IPv6 governance structure and to effectively govern and enforce IPv6 transition efforts for GSA enterprise. The IPv6 IPT is led by the Deputy Chief Information Officer (DCIO) and includes representatives from the Federal Acquisition Service's Technology Transformation Services and Office of IT Category and various divisions within GSA IT that are supportive of IPv6 transition efforts with all services and staff offices. All questions concerning IPv6 transition may be addressed to the IPT via ipv6@gsa.gov.

7. References.

a. OMB Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6), November 19, 2020.

b. OMB Memorandum M-17-06, Policies for Federal Agency Websites and Digital Services, November 8, 2016.

c. GSA Order CIO 2160.1F CHGE 2, GSA Information Technology (IT) Standards Profile, March 31, 2017.

d. GSA Order CIO 2100.1M, GSA Information Technology (IT) Security Policy, March 26, 2021.

e. GSA Order CIO 2101.2, GSA Enterprise Information Technology Management (ITM) Policy, September 3, 2019.

f. GSA Order CIO 2110.4 CIO, Enterprise Architecture Policy, May 24, 2017.

g. OMB Circular A-130, Managing Information as a Strategic Resource, Revised July 28, 2016.

h. NIST Special Publication (NIST SP) - 500-267Ar1, National Institute of Standards IPv6 Standards Profile, November 24, 2020.

i. NIST SP 500-267Br1, National Institute of Standards USGv6 Profile, November 24, 2020

j. NIST SP 500-281Ar1, National Institute of Standards USGv6 Test Program Guide, November 24, 2020

k. NIST SP 500-281Br1, National Institute of Standards USGv6 Test Methods: General Description and Validation, November 24, 2020.

l. NIST SP 800-119, National Institute of Standards Guidelines for the Secure Deployment of IPv6, November 24, 2020

m. NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations, September 2020 (includes updates as of December 10, 2020).

n. General Services Acquisition Manual (GSAM), 511.170 Information Technology Coordination and Standards.

o. GSAM, 539.101 Policy

p. Federal Acquisition Regulations, (FAR) 11.002(g)

8. Signature.

/S/_____
DAVID SHIVE
Chief Information Officer
GSA IT

Last Reviewed: 2021-05-17