GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2120
5/26/2022

GSA ORDER

SUBJECT: Internet Protocol Version 6 (IPv6) Policy

1. Purpose. This order provides acquisition and IT policy for the General Services Administration (GSA) on the provisioning of products and services, and the continued transition, implementation and use of the next generation of the Internet Protocol (IP), which is the primary protocol that serves as the building block of nearly all information and communication technology (IT or ICT) and operational technology (OT).

The next-generation Internet Protocol, known as IPv6, is necessary due to the worldwide exhaustion and inherent security, operational and performance (i.e., user experience) limitations of the more prominent Internet Protocol version 4 (IPv4). Proactive integration of IPv6 requirements into GSA contracts reduces the costs and complexity of transition by ensuring that Federal applications can operate in an IPv6 environment without costly upgrades.

This order directly addresses and incorporates applicable federal policies, standards, and guidelines, including roles and responsibilities, the GSA Acquisition Manual (GSAM), and FAR 39.101(d).

2. Cancellation. This Order cancels and supersedes Instructional Letter CIO IL-21-01 Internet Protocol Version 6 (IPv6) Policy dated May 17, 2021.

3. Explanation of Changes.

a. Updated policy references and links;

b. Expanded applicability section to include information about each role;

c. Updated roles and responsibilities, and

d. Incorporated guidance and similar program goals of the zero-trust networking initiative.

4. Background.

a. In November 2020, the Office of Management and Budget (OMB) issued OMB Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6), requiring federal agencies to complete the transition to IPv6 and retire the use of IPv4 - namely on internal network infrastructure. While M-21-07 rescinded previous OMB memorandums, the following elements remain applicable: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.

b. Since 2006, the Federal Acquisition Regulation (FAR) has incorporated IPv6 acquisition requirements as a result of the previous OMB memoranda on IPv6. This long-time transition to IPv6 is increasingly necessary due to the inability of IPv4 to meet the Government's long-term business needs because of limited robustness, scalability, and features.

5. Applicability.

a. This IPv6 policy applies to all activities and contracts for supplies, products, and services associated with information and communications technology (IT and/or ICT), operational technology (OT or “Internet of Things”), and associated digital services. This order directly addresses and incorporates applicable Federal policies, standards, and guidelines, including roles and responsibilities. This order applies to you:

(1) the IT system owner—when writing your acquisition plan, conducting market research and description of agency needs, in accordance with FAR 7.105(b)(4) and FAR 12.202.

(2) the contracting officer (CO)—for all IT and ICT-related acquisitions of products and services, in accordance with GSAM 511.170(e) and 511.171. unless otherwise indicated. CO’s must include compliance with this policy in the contract or task order for contractor employees.

(3) the IT service provider (i.e., government and contractor teams)—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.

(4) government and contractor teams, including but not limited to Contracting Officer Representatives (CORs), Technical Points of Contact (TPOCs) and Program Managers (PMs)—when conducting cybersecurity, development, modernization and enhancement (DME) activities, and ongoing operations and maintenance (O&M) of all IT products and services; see Section 6. Roles and Responsibilities, for more details.

b. This order 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 order 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.

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

a. Office of the Chief Technology Officer. Manages GSA's IT Standards function. Responsibilities include reviewing and approving requests for new software solutions (including the solution's IPv6 capabilities and parity with IPv4) to be added to the list of approved agency IT Standards. Responsibilities include ensuring that all new software solutions added to the list of approved software are IPv6 enabled/compliant, and current approved IPv4 software have plans to migrate to IPv6.

b. Office of the Chief Information Security Officer.

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

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

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

c. Office of Digital Infrastructure Technologies.

(1) Customer Relationship Management Division.

(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.

(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 division to ensure IPv6 cybersecurity and operational capabilities are evaluated.

(3) Infrastructure Integration Division. Designs, tests, and accepts/rejects infrastructure compute, storage and network solutions proposed by GSA IT, including ensuring the solution is 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.

(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 division to ensure cybersecurity and operational capabilities are maintained.

d. System Owners. Understand the impact of migrating to an IPv6 only environment (internal systems) and IPv4/IPv6 (public-facing or external systems), 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.

e. Technology Transformation Services. Support and champion the transition, implementation and use of IPv6 in the performance and execution of shared service delivery of and consulting services for government-wide and agency-specific solutions at the federal, state, tribal and local levels of government.

f. Contracting Officers (CO). In accordance with GSAR parts 511.170(e) and 511.171, COs must include compliance with this policy in the contract or task order for contractor employees. They must also ensure that all new acquisition activities to award contracts and task orders associated with information technology, including professional services, include:

(1) the addition of appropriate contract clauses;

(2) a requirement that the vendor(s) include the appropriate USGv6 conformance standards and attestation reports; and

(3) contract modifications to ensure that ongoing performance of the contract/task order is supportive of federal and GSA requirements, playbooks and framework requirements for IPv6 in consultation with Contracting Officer Representatives (CORs) and Program Managers.

f. IPv6 Integrated Project Team (IPT) 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 the GSA enterprise. The IPv6 IPT is led by the Deputy Chief Information Officer (DCIO) and includes representatives from the Federal Acquisition Service's TTS and Office of IT Category and various divisions within GSA IT that are supportive of IPv6 transition efforts with all services and staff offices.

7. Policies and Procedures.

a. As required by OMB 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 this memo, 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. Consistent with OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, GSA is undergoing a transition to zero trust architecture, while at the same time undergoing a transition to IPv6. GSA is coordinating the implementation of these initiatives.

(1) This GSA policy does not require commercial shared service providers (e.g., ISPs, CSPs, CDNs) to migrate their internal infrastructures to support IPv6 alone. Instead, GSA will prioritize working with shared services platforms to ensure they provide IPv6 support (i.e., dual-stack IPv4/IPv6) on the interfaces (e.g., domain names, websites, email services) exposed to the general public, system owners, and other organizations.

(2) More generally, the Federal Government's and GSA's IPv6 transition should not slow the migration to the cloud or zero trust architectures. GSA's IPv6 adoption plans and its contractor activities will and should first focus on technology areas where IPv6 support is already mature, while allowing time for other service and product providers to upgrade their offerings.

c. The National Institute of Standards and Technology's (NIST's) 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.

d. 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;

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

(5) Ensure that plans for full support for zero-trust networking incorporating IPv6 services are included in zero-trust adoption plans, IT security plans, testing and change management activities, architectures, and acquisitions.

e. All inquiries may be addressed to the agency IPv6 IPT via ipv6@gsa.gov.

8. 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. OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022.

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

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

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

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

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

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

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

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

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

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

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

o. General Services Acquisition Manual (GSAM), Describing Agency Needs—511.170 Information Technology Coordination and Standards.

p. GSAM, Acquisition of Information Technology—539.101 Policy.

q. Federal Acquisition Regulations, (FAR), Describing Agency Needs—11.002(g) Policy.

r. FAR, Acquisition Planning—7.105(b)(4) Contents of Written Acquisition Plans.

s. FAR, Acquisition of Commercial Products and Commercial Services—12.202 Market Research and Description of Agency Need.

t. FAR, Requirements for GSA Information Systems—511.171 Policy.

u. FAR, Acquisition of Information Technology—39.101(d) Policy.

9. Signature.

DocuSigned by:
David Shive
A3AE4284A2754F9...

DAVID SHIVE
Chief Information Officer
GSA IT