EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 19, 2020

M-21-07

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Completing the Transition to Internet Protocol Version 6 (IPv6)

This memorandum updates guidance on the Federal government's operational deployment and use of IPv6. IPv6 is the next-generation Internet protocol, designed to replace version 4 (IPv4) that has been in use since 1983. Internet Protocol (IP) addresses are the globally unique numeric identifiers necessary to distinguish individual entities that communicate over the Internet. The global demand for IP addresses has grown exponentially with the ever-increasing number of users, devices, and virtual entities connecting to the Internet, resulting in the exhaustion of readily available IPv4 addresses in all regions of the world. Over time, numerous technical and economic stop-gap measures have been developed in an attempt to extend the usable life time of IPv4, but all of these measures add cost and complexity to network infrastructure and raise significant technical and economic barriers to innovation. It is widely recognized that full transition to IPv6 is the only viable option to ensure future growth and innovation in Internet technology and services.[1] It is essential for the Federal government to expand and enhance its strategic commitment to the transition to IPv6 in order to keep pace with and capitalize on industry trends. Building on previous initiatives,[2] the Federal government remains committed to completing this transition.[3]

Beginning in 2005, the Federal government's IPv6 initiative served as a vital catalyst, fostering commercial development and adoption of IPv6 technology. In the last 5 years, IPv6

[1] IAB Statement on IPv6, The Internet Architecture Board, November 2016, https://www.iab.org/2016/11/07/iab-statement-on-ipv6/.

[2] 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. This policy outlined deployment and acquisition requirements. 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. Specifically, the 2010 memorandum required agencies to upgrade public/external facing servers and services (*e.g.*, web, email, DNS, ISP services) to operationally use native IPv6 by the end of FY 2012; and to and to upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014.

[3] This memorandum does not apply to national security systems, although the document may be leveraged to inform their management processes.

momentum in industry has dramatically increased, with large IPv6 commercial deployments in many business sectors now driven by reducing cost, decreasing complexity, improving security and eliminating barriers to innovation in networked information systems. Several large network operators, software vendors, service providers, enterprises, state governments, and foreign governments have deployed significant IPv6 infrastructures. In fact, many of these organizations have migrated, or are planning to migrate, to "IPv6-only"[4] infrastructures to reduce operational concerns associated with maintaining two distinct networking regimes.[5]

This memorandum communicates the requirements for completing the operational deployment of IPv6 across all Federal information systems and services, and helps agencies overcome barriers that impede them from migrating to IPv6-only network environments. The strategic intent is for the Federal government to deliver its information services, operate its networks, and access the services of others using only IPv6.[6]

Specific steps that agencies are expected to take to complete the transition to IPv6

Preparing for an IPv6-only Infrastructure

OMB previously issued policy discussing the expectation for agencies to run dual stack (IPv4 and IPv6) into the foreseeable future; however, in recent years it has become clear that this approach is overly complex to maintain and unnecessary. As a result, standards bodies and leading technology companies began migrating toward IPv6-only deployments, thereby eliminating complexity, operational cost, and threat vectors associated with operating two network protocols.

In many instances where Federal agencies deployed IPv6 on public facing systems, IPv6 access is already being used by as many, or more, users as IPv4. As information technology continues to evolve toward mobile platforms, Internet of Things (IoT), and wireless networks, IPv6 growth will continue to accelerate.

The technical, economic and security benefits of operating a single, modern, and scalable network infrastructure are the driving forces for the evolution towards IPv6-only in the private sector. To keep pace with and leverage this evolution in networking technology, agencies shall:

1. Designate an agency-wide IPv6 integrated project team (including acquisition, policy, and technical members), or other governance structure, within 45 days of issuance of this policy to effectively govern and enforce IPv6 efforts;

[4] IPv6-only refers to the state of an operational system or service when IPv4 protocol functions (addressing, packet forwarding) are not in use. The NIST USGv6 profile defines technical requirements for a product to be capable of operating in IPv6-only environments.

[5] Examples of industry trends in IPv6 migration can be found at: https://www.internetsociety.org/deploy360/ipv6/case-studies/ and https://teamarin.net/get6/ipv6-case-studies/.

[6] Note that for public Internet services, maintaining viable IPv4 interfaces and transition mechanisms at the edge of service infrastructures may be necessary for additional time, but this does not preclude operating the backend infrastructure as IPv6-only.

2. Issue and make available on the agency's publicly accessible website, an agency-wide IPv6 policy, within 180 days of issuance of this memorandum. The agency-wide IPv6 policy must require that, no later than Fiscal Year (FY) 2023, all new networked Federal information systems are IPv6-enabled[7] at the time of deployment, and state the agency's strategic intent to phase out the use of IPv4 for all systems;

3. Identify opportunities for IPv6 pilots and complete at least one pilot of an IPv6-only operational system by the end of FY 2021 and report the results of the pilot to OMB upon request;[8]

4. Develop an IPv6 implementation plan[9] by the end of FY 2021, and update the Information Resources Management (IRM) Strategic Plan[10] as appropriate, to update all networked Federal information systems (and the IP-enabled assets associated with these systems) to fully enable native IPv6[11] operation. The plan shall describe the agency transition process and include the following milestones and actions:[12]

    a. At least 20% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2023;[13]
    b. At least 50% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2024;
    c. At least 80% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2025; and
    d. Identify and justify Federal information systems that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems;

[7] IPv6-enabled refers to a system or service in which the use of IPv6 is "turned on" for production use.

[8] In order to expedite progress towards IPv6-only enterprise deployments, NIST, through the National Cyber Center of Excellence (NCCoE), will establish a cooperative Federal government and industry pilot project to the demonstrate commercial viability and to document a practice guide for secure IPv6-only enterprise deployment scenarios.

[9] The IPv6 implementation plan must ensure coordination with other, relevant department modernization initiatives and require that all shared services offered by the agency provide full IPv6 support (including the ability to function in IPv6-only mode) with feature and performance parity with existing IPv4 services.

[10] Agencies are required to maintain an IRM Strategic Plan in accordance with OMB Circular A-130, *Managing Information as a Strategic Resource*.

[11] Native IPv6 refers to direct support of IPv6 in a system or service without requiring the use of IPv4 for basic communications.

[12] OMB guidance has required agencies to acquire and deploy IPv6 capabilities in some systems since 2010. It is recommended that agencies inform the development of their plan with practical experience gained from pilot activities and prior production deployments. Agency plans will evolve over time and thus it is important to identify systems that are already capable of running IPv6 and develop and implement plans to enable IPv6 in those systems first, then evaluate the potential to migrate those systems to IPv6-only environments.

[13] Potential starting points might include enabling IPv6 on existing systems that are already capable of running IPv6 (*e.g.*, focusing on commodity IT systems with commercial off the shelf operating systems that are already capable of running IPv6.)

5. Work with external partners to identify systems that interface with networked Federal information systems and develop plans to migrate all such network interfaces to the use of IPv6; and

6. Complete the upgrade of public/external facing servers and services (*e.g.*, web, email, DNS, and ISP services) and internal client applications that communicate with public Internet services and supporting enterprise networks to operationally use native IPv6.

Adhering to Federal IPv6 Acquisition Requirements

In December 2009, the Federal Acquisition Regulation (FAR) Council issued a final rule amending the FAR[14] to ensure that future acquisitions of networked information technology included IPv6 requirements. The key element of this amendment states:

- "Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program."

This strategic acquisition approach enables natural technology refresh cycles to upgrade the installed base of networked IT products and services to be IPv6-capable.[15] Doing so ensures that Federal IT systems are positioned to leverage the technical and economic benefits of IPv6, and enable Federal Chief Information Officers to eventually migrate to IPv6-only environments when appropriate. In accordance with existing FAR requirements, agencies shall:

1. Continue to use the USGv6 Profile to define agency or acquisition specific requirements for IPv6 capabilities when purchasing networked information technology and services. Going forward, this should include specifying the requirement for hardware and software to be capable of operating in an IPv6-only environment;

2. Continue to require potential vendors to document compliance with such IPv6 requirement statements through the USGv6 Test Program; and

3. In rare circumstances where requiring demonstrated IPv6 capabilities would pose undue burden on an acquisition action, provide a process for agency Chief Information Officers 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.

[14] The IPv6 FAR Requirements can be located at: https://www.gpo.gov/fdsys/pkg/FR-2009-12-10/html/E9-28931.htm.

[15] IPv6-capable refers to a system or service that has correctly implemented a complete set of IPv6 capabilities. The NIST USGv6 profile describes detailed technical requirements for IPv6 capabilities for distinct product types.

Evolving the USGv6 Program

In order to continue to protect Federal investments in IPv6 technology and to ensure the quality and completeness of IPv6 capabilities in acquisitions, NIST will continue to update and expand the USGv6 Program. NIST will continue to issue periodic updates to the USGv6 Profile to incorporate the latest Internet Engineering Task Force (IETF)[16] specifications relevant to IPv6 technology. Special emphasis shall be placed on ensuring the inclusion of IPv6 security technologies and those network capabilities necessary to support other Federal initiatives such as IoT, adoption of cloud-based shared services, advanced wireless communications, and software defined and virtualized networks.

The USGv6 Test Program will continue to provide government-wide conformance and general interoperability testing of commercial product offerings. This program will continue to be implemented by accredited external testing laboratories and continue to be 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, agencies shall:

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 focus on specific systems integration, performance and information assurance testing not covered in the USGv6 Test Program.

Ensuring Adequate Security

In addition to Federal guidance, industry guidance and best practices for the secure deployment of IPv6 have been well documented.[17] While the knowledge base of how to secure IPv6 has matured significantly, the understanding of how IPv6 enables more efficient approaches to overall security is often overlooked. For example, organizations that develop IPv6 addressing plans that are highly correlated with their network security architecture are finding a significant reduction in the complexity of their security configurations. In order to help realize these security benefits across the Federal government, agencies shall:

1. Ensure that plans for full support for production IPv6 services are included in IT security plans, 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;

[16] For additional information on the IETF, refer to https://www.ietf.org/.

[17] Examples include: IPv6 Enterprise Network Scenarios at https://datatracker.ietf.org/doc/rfc4057/; Enterprise IPv6 Deployment Guidelines at https://datatracker.ietf.org/doc/rfc7381/; IPv6 Transition/Co-existence Security Considerations at https://datatracker.ietf.org/doc/rfc4942/; and other specifications from the IETF IPv6 Operations (v6Ops) and Operational Security Capabilities for IP Network Infrastructure (OpSec) working groups at https://datatracker.ietf.org/wg/v6ops/about/ and https://datatracker.ietf.org/wg/opsec/about/.

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.

Government-wide Responsibilities

The following agencies lead Government-wide efforts to support the transition to IPv6.

The Department of Commerce will:

1. Continue to enhance and maintain the USGv6 Profile and Test program; and

2. Develop, in collaboration with the Department of Homeland Security, enhanced security guidelines for IPv6 adoption throughout the Federal IT infrastructure.

The Department of Homeland Security will:

1. Develop, in collaboration with the Department of Commerce, enhanced security guidance and operational directives for IPv6 adoption throughout the Federal IT infrastructure;

2. Enhance relevant security and resilience programs and services (*e.g.*, Trusted Internet Connections, Continuous Diagnostics and Mitigation, Einstein) to fully support the production use of IPv6 in all Federal IT systems; and

3. Enhance the ability to measure and report on the extent of IPv6 and IPv4 deployment and utilization levels within Federal information systems.

The General Services Administration will:

1. Ensure relevant GSA programs and services require full IPv6 support with feature and performance parity with existing IPv4 services;

2. Ensure that government-wide contract vehicles include IPv6 requirements for acquisitions using Internet Protocol; and

3. Work with agencies and Enterprise Infrastructure Solutions (EIS) vendors to ensure that all EIS network services are IPv6-enabled at the time of deployment as specified by agency IPv6 implementation plans and EIS task orders.

The Federal Chief Information Officer's Council, in collaboration with the Federal Chief Acquisition Officer's Council, will:

1. Support OMB and the agencies by providing guidance for IPv6 implementation, as necessary;

2. Provide for an interagency forum to share information and best practices, and coordinate efforts with external partners, as appropriate, in support of the transition to IPv6; and

3. Engage with industry, as appropriate, to obtain lessons learned and best practices and ensure that products and services meet the needs of the Federal government.

Rescissions

This memorandum rescinds M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*, August 2, 2005 and *Transition to IPv6*, September 28, 2010. The 2010 memorandum required Federal agencies to operationally deploy native IPv6 for public Internet servers and internal applications that communicate with the public servers. While the 2010 memorandum is now rescinded, the following two actions from the 2010 memorandum are still relevant and agencies are required to address them in future agency IPv6 transition plans and reports: (1) upgrade public/external facing servers and services (*e.g.*, web, email, DNS, ISP services, etc.) to operationally use native IPv6 by the end of FY 2012; and (2) upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014. While the 2012 and 2014 deadlines have past, OMB expects agencies who have not yet completed these actions to do so as soon as possible.

Policy Assistance

All questions or inquiries should be addressed to the OMB Office of the Federal Chief Information Officer (OFCIO) via email: ofcio@omb.eop.gov.