MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Acting 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 Internet's next-generation protocol, designed to replace version 4 (IPv4) that has been in use since 1983. Internet Protocol (IP) addresses are the unique, global numeric identifiers necessary to identify individual entities that communicate over the Internet. In 2015 the available free pool of IPv4 addresses was exhausted as the global demand for IP addresses has grown exponentially with the ever-increasing number of users, devices, and virtual entities connecting to the Internet. 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, the Federal government remains committed to completing its transition to IPv6.[2]

Beginning in 2005, the Federal government's IPv6 initiative served as a vital catalyst, fostering commercial development and adoption of IPv6 technology.[3] 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] This memorandum does not apply to national security systems, although agencies may leverage the document to inform their management processes.

[3] 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, etc.) to operationally use native IPv6 by the end of FY 2012; 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.

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 network infrastructures.

The intent of this updated memorandum is to communicate the requirements for completing the operational deployment of IPv6 across all Federal information systems and services, and help agencies overcome barriers that prevent them from migrating to IPv6-only systems. Going forward, the Federal government plans to deliver its information services, operate its networks, and access the services of others using only IPv6.

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,[5] 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 being used by as many users as IPv4. As information technology continues to evolve toward mobile platforms and wireless networks, IPv6 growth will continue to accelerate for such services.

Several large networks and data centers have already evolved their internal infrastructures to be IPv6-only. Forward looking large corporations are also working toward migrating their enterprise networks to IPv6-only environments. The technical, economic and security benefits of operating a single, modern, and scalable network infrastructure are the driving forces for such evolution in the private sector. To keep pace with and leverage this evolution in networking technology, agencies shall:

[4] IPv6-Only refers to network environments in which use of the IPv4 protocol has been eliminated.

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

1. Designate an integrated agency-wide IPv6 team, or other governance structure, within 45 days of issuance of this policy, in support of the agency's Enterprise Risk Management capability to effectively govern and enforce IPv6 efforts;

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 FY 2023, all new networked Federal information systems are IPv6-enabled prior to being made operational, and outline a plan to phase out use of IPv4 for all systems by either converting to IPv6-only or replacing or retiring 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;[6]

4. Develop an IPv6 implementation plan by the end of FY 2021, and update the Information Resources Management (IRM) Strategic Plan[7] as appropriate, to improve all networked Federal information systems (and the IP-enabled assets associated with these systems) to fully enable native IPv6 operation.[8] The plan shall describe your transition process and include the following milestones and actions:

    a. At least 20% of IP-enabled assets on Federal networks are IPv6-only by the end of FY 2023;[9]

    b. At least 50% of IP-enabled assets on Federal networks are IPv6-only by the end of FY 2024;

    c. At least 80% of IP-enabled assets on Federal networks are IPv6-only by the end of FY 2025; and

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

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

[8] To support the IPv6 implementation plan, agencies are expected to continue to require demonstrated IPv6 capabilities in acquisitions to evolve the installed base to become fully IPv6 capable. This will enable agencies to pursue an incremental approach to their planning and deployment. Rather than waiting until the agency IPv6 plan and detailed deployment plans for all systems are established, agencies should identify systems that are the most straightforward and develop and implement plans to enable IPv6 in those systems, then evaluate the potential to migrate those systems to IPv6-only environments.

[9] Potential starting points might include enabling IPv6 on existing systems that are already IPv6-capable (e.g. focusing on commodity IT systems with IPv6-capable commercial off the shelf operating systems; completing the deployment of IPv6 on all Internet facing services; and building upon prior OMB guidance by expanding the scope of IPv6 to additional internal systems that communicate with the Internet.) With the experience gained from initial deployments, agencies can develop detailed system plans for IPv6 deployment in remaining systems.

d. Identify and justify Federal information systems that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems;

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

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

Adhering to Federal Acquisition Requirements

In December 2009, the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council issued a final rule amending the Federal Acquisition Regulation (FAR)[10] to:

- Require all acquisitions of networked information technology and services to include IPv6 requirements expressed using National Institute of Standards and Technology (NIST) Special Publication 500-267B, "*USGv6 Profile*"; and
- Require vendors to document their compliance with those requirements in accordance with the USGv6 Test Program as outlined in NIST Special Publication 500-281A, "*USGv6 Test Program Guide."*[11]

This acquisition approach created a strategic focus on natural technology refresh cycles to upgrade the installed base of networked IT products and services. Doin so will ensure that Federal IT systems are positioned to leverage the technical and economic benefits of IPv6, and enable Federal CIOs to eventually migrate to IPv6-only environments where appropriate. In accordance with existing FAR requirements, agencies shall:

1. Continue to include explicit requirements for IPv6 capabilities in all acquisitions of common networked information technology and services, this includes specifying the need for hardware and software to be capable of operating in an IPv6-only environment (as opposed to dual-stack) in acquisitions going forward. These requirements must be expressed using the USGv6 Profile and include the requirement to demonstrate compliance with those requirements through the USGv6 Test Program; and

2. In rare circumstances where requiring demonstrated IPv6 capabilities would pose undue burden on an acquisition action, provide a process for agency CIOs 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.

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

[11] USGv6 Profile and Test Program is documented at: https://www.nist.gov/programs-projects/usgv6-program.

Leveraging the NIST 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 is updating and expanding the USGv6 Program. NIST will continue to issue periodic updates to the USGv6 Profile to incorporate the latest Internet Engineering Task Force (IETF)[12] specifications relevant to IPv6 technology. Special emphasis shall be placed on ensuring the inclusions of IPv6 security technologies and those network capabilities necessary to support other Federal initiatives such as Internet of Things, adoption of cloud based shared services, advanced cellular communications, and software defined and virtualized networks. Additional enhancements to the USGv6 program will enable the explicit specification and test of requirements for products to support operation in IPv6-only environments.

NIST's updates to the USGv6 Test Program will also provide government-wide conformance and 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 leverage the USGv6 Profile and Test Program as part of their acquisition strategy. Specifically, agencies shall:

1. Use the USGv6 Profile to define agency or acquisition specific requirements for IPv6 capabilities in commercial products; and
2. Rely on the USGv6 Test Program for basic conformance and interoperability testing of commercial products. Agency or acquisition specific testing should focus on detailed 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.[13] 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

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

[13] 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/; Operational Security Considerations for IPv6 Networks at https://datatracker.ietf.org/doc/draft-ietf-opsec-v6/; and Recommendations on the Filtering of IPv6 Extension Headers at https://datatracker.ietf.org/doc/draft-ietf-opsec-ipv6-eh-filtering/.

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 all IT security plans, architectures and acquisitions;

2. Ensure that all systems that support 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 capable of operating in IPv6-only environments; and

3. Follow applicable Federal guidance[14] and industry leading practice guidance for the secure deployment and operation of IPv6 networks.

Government-wide Responsibilities

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

The Department of Commerce is responsible for the following actions:

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 is responsible for the following actions:

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 is responsible for the following actions:

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

[14] For example, NIST Special Publication 800-119, *Guidelines for the Secure Deployment of IPv6*.

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.

The Federal Chief Information Officer's Council is responsible for the following actions:

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 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 by XYZ.

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.