Frequently Asked Questions (FAQs)

Overview of Federal IPv6 Task Force

The Federal IPv6 Task Force, established by the Federal Chief Information Officers Council (CIOC), is committed to communicating frequently with Federal agencies, industry, and other stakeholders on IPv6-only adoption progress among Federal agencies. This publicly available Frequently Asked Questions (FAQ) document provides stakeholders with common questions regarding the Federal government's adoption of Internet Protocol version 6 (IPv6) and their answers or required clarifications.

Stay Connected: The IPv6 Federal Task Force communicates across several existing listservs. We encourage you to register for the public email list called the Fedv6-Deploy distribution list. To subscribe, send an email to: fedv6-deploy+subscribe@list.nist.gov. Additionally, we recommend that you register to join the Cloud & Infrastructure Community of Practice (C&I CoP). The C&I CoP team (GSA) also serve as the Managing Partner of the IPv6 Federal Task Force and regularly communicate about IPv6 and other topics of interest to its members. To join the C&I CoP, send an email message from a .gov or .mil email address only to listserv@listserv.gsa.gov to join the DCOI listserv/CoP.

Additional Resources: For Federal staff, additional resources, including templates, tools, and training resources are available on the IPv6 Federal Task Force OMB MAX Webpage. These materials are available to those with .gov or .mil email addresses.

Contact: To contact the IPv6 Federal Task Force, please reach out to fedv6-exec@list.nist.gov.

Questions and Answers

Question 1: Are commercial shared service providers that sell to the Federal Government expected to be in alignment with the IPv6-only milestones laid out in M-21-07?

Answer: M-21-07 does not intend to require commercial shared service providers (e.g. ISPs, CSPs, CDNs) to migrate their internal infrastructures to only support IPv6. Instead, agencies should prioritize working with shared services platforms to ensure they provide IPv6 support on the interfaces exposed to system owners and other organizations. More generally, the federal government's IPv6 transition should not slow the migration to the cloud or zero trust architectures.

More generally, the federal government's IPv6 transition should not slow near term progress on other federal IT initiatives (e.g., migration to cloud, zero trust architectures). Where product / service offerings necessary to implement these other initiatives are lacking in IPv6 support, the requirements for IPv6 capabilities in future product releases should be explicitly stated and specific technology roadmaps to address those requirements should be solicited from vendors.

Question 2: What resources are available to vendors that are interested in selling IPv6 products to the Federal Government?

Answer: Vendors wishing to sell products to the Federal government can avail themselves of the services of the USGv6 Test Program – to document the detailed IPv6 capabilities of their products and to demonstrate their conformance to international standards and their interoperability with other vendor products. GSA also provides solutions with vendors utilizing IPv6 products and IPv6 capable ISPs. Please visit: https://www.gsa.gov/technology/technology-products-services/it-security for more information.

Question 3: Does the Federal Government provide standardized language for agencies to assist in the governmentwide acquisition of IPv6 products and services?

Answer: In accordance with the Federal Acquisition Regulation (FAR) 11.002 (g), contracting officers must include IPv6 requirements in all contracts and orders for information technology that will have the capability to access the Internet or any network utilizing Internet Protocol (IPv4 or IPv6).

The USGv6 Profile provides a vocabulary for expressing the IPv6 capability requirements of common IT products.

To assist agencies, the Federal IPv6 Task Force is collecting examples of language that agencies have used successfully. The Task Force is compiling these examples and will plan to release best practices to all Federal agencies via OMB MAX. If you have examples of successful IPv6 acquisition language, please email these to lee.ellis@gsa.gov.

Question 4: How should agencies coordinate their adoption of ZTA (Zero Trust Architecture) and their transition to IPv6?

Answer: Federal agencies are undergoing a transition to IPv6, as described in OMB Memorandum M-21-07, while at the same time migrating to a ZTA. Agencies should coordinate the implementation of these initiatives when they revisit their enterprise network infrastructure and policies. Conceptually, ZTAs should be protocol agnostic. The reality is that products purchased to implement zero trust must support both IPv4 and IPv6. For example, if an Agency purchases a Zero Trust product that only works on IPv4, then the agency may have to use legacy/alternative methods to support the IPv6 assets that are being rolled out in accordance with M-21-07.

Question 5: What existing resources are available for the testing and monitoring of IPv6 deployment?

Answer: The USGv6 Test Program provides means to test the capabilities, correctness and interoperability of products before they are deployed. Several informal test and measurement services track aspects of IPv6 deployment in various sectors of the Internet, including:

- NIST IPv6 Deployment Monitor - https://fedv6-deployment.antd.nist.gov/

- Test-IPv6 - https://test-ipv6.com/

Question 6: When will FedRAMP begin to require IPv6 for products?

Answer: FedRAMP is already requiring offerings to support agencies in meeting their IPv6 requirements. Cloud service providers must support these requirements by providing systems that can operate using only IPv6 connectivity to agency implementations and their customers. The FedRAMP team is also working with acquisition and NIST officials to meet requirements of posted guidance, from DHS CISA, OMB and NIST. That said, it is still essential that agencies adhere to the Federal Acquisition Regulation by including IPv6 requirements in all contracts and orders for information technology that will have the capability to access the Internet or any network utilizing Internet Protocol.

Question 7: How many IPv6 test labs/beds have been or will be established?

Answer: Test labs for the USGv6 program are accredited to ensure that they are proficient in using the standardized test methods of the program and its reporting requirements. Currently there is one accredited test lab in the program, the Interoperability laboratory at the University of New Hampshire (IoL). UNH IoL is also the North American test lab for the IPv6 Ready Logo program, USGv6 Test Program and the IPv6 Ready Logo program are highly aligned such that most vendors pursue both test programs in one visit. Questions about the USGv6 Program can be addressed to: usgv6-program@list.nist.gov.

Question 8: How can agencies leverage the USGv6 Profile and Test Program in acquisitions?

Answer: The USGv6 Profile and Test Program was designed to support USG acquisition of IPv6 capable products. The profile provides a vocabulary for expressing the technical requirements for IPv6 capabilities in commercial products. The test program provides a means to have independent laboratories test the completeness, correctness, and interoperability of IPv6 capabilities found in commercial products. To leverage these services – incorporate USGv6-based requirement statements in solicitations for networked products and services and require the submission of USGv6 test results as part of the vendor's response to the solicitation. It is up to the acquisition PoC to compare the test results to the specific solicitation requirements to ensure their alignment.

Question 9: What are DoD's intentions with respect to transitioning to IPv6-only?"

Answer: DoD is committed to the complete implementation of IPv6 and to accomplishing all of the requirements in M-21-07. In Fiscal Year 2021, DoD published its IPv6 policy in Directive-Type Memorandum 21-004, DoD Implementation of IPv6. In addition, DoD completed and reported an IPv6-only pilot and published its IPv6 Implementation Plan, covering the requirements of M-21-07. DoD recognizes the need to begin by establishing a dual stack IPv4/IPv6 enterprise across all DoD networks as an evolutionary step to realizing an IPv6-only network. For more information on DOD

IPv6 implementation efforts visit: Department of Defense Implementation of Internet Protocol Version 6.