








UNITED STATES
FEDERAL COMMUNICATIONS COMMISSION
INFORMATION TECHNOLOGY

FCC INFORMATION TECHNOLOGY (IT) INTERNET PROTOCOL VERSION 6 (IPV6) COMPLIANCE POLICY

OFFICE OF THE MANAGING DIRECTOR

45 L Street NE, Washington, DC 20554

Record of Approval

| Document Approval | |
|--|---------------------------|
| <Document POC> | |
| Printed Name: Arecio Dilone (ACIO-D&P) | |
| Signature:  Digitally signed by Arecio Dilone Date: 2021.04.21 11:40:14 -04'00' | Date: 4/21/2021 |
| <Approval Structure> | |
| Printed Name: Mark Stephens (Managing Director) | |
| Signature:  Digitally signed by Mark Stephens Date: 2021.04.22 15:45:49 -04'00' | Date: |
| Printed Name: Francisco Salguero (CIO) | |
| Signature:  Digitally signed by FRANCISCO SALGUERO DN: c=US, o=U.S. Government, ou=Federal Communications Commission, cn=FRANCISCO SALGUERO, 0.9.2342.19200300.100.1.1=27001000021809 Date: 2021.04.22 12:08:09 -04'00' Adobe Acrobat Reader version: 2021.001.20149 | Date: |
| Printed Name: Jennifer Bilbrey (DCIO-M/L) | |
| Signature:  Digitally signed by Kevin Baker DN: cn=Kevin Baker, o, ou, email=kevin.baker@fcc.gov, c=US Date: 2021.04.21 11:58:30 -04'00' | Date: 4/21/2021 |
| Printed Name: Andrea Simpson (CISO) | |
| Signature: ANDREA SIMPSON Digitally signed by ANDREA SIMPSON DN: c=US, o=U.S. Government, ou=Federal Communications Commission, cn=ANDREA SIMPSON, 0.9.2342.19200300.100.1.1=27001002878969 Date: 2021.04.21 13:13:14 -04'00' | Date: |
| Printed Name: Shaun Costello (DCIO-T/R) | |
| Signature:  Digitally signed by Shaun Costello Date: 2021.04.22 11:51:14 -04'00' | Date: |

Revision Log

| Date | Description | Author |
|------------|---------------------------------------|------------------|
| 11/30/2020 | First Draft | Arecio Dilone |
| 03/30/2021 | Second Draft, with updates from OCIOs | IT Data & Policy |
| 4/21/2021 | Final | Arecio Dilone |
| | | |
| | | |
| | | |

Table of Contents

| | |
|--|----------|
| RECORD OF APPROVAL | 1 |
| REVISION LOG | 2 |
| 1. INTRODUCTION | 4 |
| 1.1. PREPARING FOR AN IPV6-ONLY INFRASTRUCTURE | 4 |
| 1.2. SCOPE | 4 |
| 1.3. PROCEDURE OR DESCRIPTION | 4 |
| 1.4. AUDIENCE | 5 |
| 2. BACKGROUND | 5 |
| 2.1. POLICY..... | 5 |
| 2.2. ROLES AND RESPONSIBILITIES | 7 |
| 2.3. WAIVERS | 8 |
| REFERENCE DOCUMENTS | 8 |
| APPENDIX A: DEFINITIONS | 9 |

1. Introduction

Beginning in 2005, the Federal government's Internet Protocol version 6 (IPv6) initiative served as a vital catalyst, fostering commercial development and adoption of IPv6 technology. In the last 5 years, IPv6 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" infrastructures to reduce operational concerns associated with maintaining two distinct networking regimes.

1.1. 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.

OMB has issued [M-21-07, "Completing the Transition to internet Protocol Version 6 \(IPv6\)"](#) which requires agencies to develop an IPv6 implementation plan by the end of FY 2021, update their Information Resources Management (IRM) Strategic Plan as appropriate, and to update all networked Federal information systems (and the IP-enabled assets associated with these systems) to fully enable native IPv6 operation. The plan shall describe the agency transition process and include the following milestones and actions:

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

1.2. Scope

This policy applies to all new FCC acquisitions of IT products or services using Internet Protocol (IP). Additional specifics are found in the IPv6 IT Procurement Checklist.

1.3. Procedure or Description

This FCC IPv6 Policy is a living document that should be reviewed and updated as new policies, memorandums and procedures are defined and approved, along with any other relevant materials.

1.4. Audience

The audience for this policy includes, but is not limited to, FCC employees whom may seek to design, build or procure a networked IT product or service, vendors responding to Requests for Proposal (RFP), and acquisition staff involved in the procurement process.

2. Background

On December 10, 2009, the Federal Acquisition Regulation (FAR) was updated to require that all new IT acquisitions using IP must be IPv6 compliant. IPv6 replaces Internet Protocol version 4 (IPv4), and it is the most recent version of IP that provides an identification and location system for computers on networks and routes traffic across the Internet. Federal agencies are required to ensure IPv6 compliance when procuring networked IT products.

On September 28, 2010, the Office of Management and Budget (OMB) issued a memorandum detailing the federal government's commitment to the operational deployment and use of IPv6 and provided guidance to ensure agency procurements comply with FAR requirements.

Some vendors have not implemented IPv6 with the same functionality as IPv4. To address this issue, the National Institute of Standards and Technology (NIST) developed the U.S. Government v6 Profile (USGv6) and defined it in the [NIST Special Publication \(SP\) 500-267B Rev1](#).

NIST SP 500-267B groups IT capabilities by the following: hosts, routers; network protection products; switches; and applications and services. The FCC will use an IPv6 profile document to specify IPv6 requirements when evaluating potential procurements. Vendors shall supply respective Supplier's Declarations of Conformity (SDoCs) to prove their products meets the IPv6 requirements.

FAR Part 11.002(g) states the requirements documents for IT equipment using IP must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST SP 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. Any exceptions to the use of IPv6 require the Chief Information Officer (CIO) to provide written approval. Sufficient details supporting the waiver must be included in the request (e.g., prohibitive cost or scheduling conflicts).

2.1. Policy

This policy implements the requirements of FAR Part 11.002(g) and requires all new FCC acquisitions of IT products or services that use IP to be IPv6 compliant and capable of functioning in an IPv6-only environment.

FCC is implementing these requirements in accordance with the guidance that OMB provided, and FCC's IPv6 requirements align with the federal goals contained in that document.

FCC requirements conform to the overall intent of the U.S. Government (USG) deployment of IPv6 to improve operational efficiency, provide the general public with continued access to citizen services and ensure the government is capable of accessing IPv6-only services.

A requestor in an Bureau or Office (B/O) seeking to procure an IT product or service using IP must work with the respective Contracting Officer (CO) to ensure appropriate IPv6 requirements language is included in the procurement package.

FCC IT urges requestors to conduct as much research as possible when evaluating IPv6 readiness with potential procurements. Requestors should consider the following resources to facilitate informed decision:

- ISP and Internet services websites should provide IPv6 information
- [Http://www.ipv6ready.org/](http://www.ipv6ready.org/) provides lists of IPv6-ready components, searchable by device type, nation, and other criteria
- New computer equipment and software may have the “IPv6 Ready” logo on its packaging, as well as relevant information within owner’s manuals, typically in the technical specifications section
- FCC’s own [Consumers Guide](#) for IPv6

A requestor in an FCC B/O office seeking to procure an IT product or service using IP shall follow FAR 11.002(g). This checklist is a guide to help ensure that products and services that use IP provide full feature functionality in both dual stack (IPv4 and IPv6) and IPv6-only environments in compliance with the NIST USGv6 Testing Program.

The requestor provides the IPv6 IT Procurement Checklist to the CO during the RFP, RFQ (Request for Quote), or RFI (Request for Information) development to ensure IPv6 requirements are included in the standard language section of the RFP.

FAR 11.002(g) specifies that agency requirement documents must include the appropriate IPv6 compliance requirements in accordance with the Agency’s Enterprise Architecture, unless a waiver to the use of IPv6 has been granted. FCC shall include the appropriate IPv6 compliance requirements consistent with FAR 11.002(g) regarding information technology acquisitions using Internet Protocol.

A vendor, when responding to a request for an IT service or product using IP, must complete and return a signed SDoC to the requestor. The requestor will conduct a technical evaluation of the vendor's proposal, analyzing the requirements and the IPv6 capabilities as captured on the SDoC. Once completed, the requestor will send the analysis to the CO.

The requestor must notify the CO of all contract specifications that do not comply with providing full feature functionality for IPv6 and act in accordance with the instructions of the CO.

When the FCC procures an IT service or product that uses IP via the Federal Schedule, sole source, or credit card, the FCC requestor is responsible for requesting the vendor SDoC if the planned procurement is not yet IPv6 capable, or certification of IPv6 capability if applicable.

2.2. Roles and Responsibilities

1. **Chief Information Officer (CIO)**
 - Approves or disapproves all IPv6 compliance waivers to this policy.
2. **Deputy CIO Infrastructure & End User Technology**
 - Receives IPv6 waiver requests.
 - Recommends approval/disapproval of IPv6 waiver requests to CIO.
3. **ACIO Budget & Acquisition**
 - Ensure the requirement for vendor IPv6 compliance has been documented appropriately in the acquisition package.
 - Verify CI&C/Engineering's IPv6 compliance review and sign-off is attached; approve or deny as appropriate (component of the Procurement Checklist).
4. **FCC Field Offices Representative**
 - Submit IPv6 waiver requests from their Program Offices or Regions.
5. **FCC Staff Requesting Procurement of IT Products or Equipment**
 - Include appropriate IPv6 requirements language in PRs and APPs.
 - Work with CO to ensure appropriate IPv6 requirements language is included in SOWs, RFPs and awarded contracts.
 - Complete IPv6 IT Procurement Checklist and send to CO.
 - Analyze the requirements, the IPv6 requirements and the product's capabilities as captured on the SDoC and submit analysis to CO.
 - If procured via federal schedule, sole source or credit card, then obtain SDoC from vendor and submit SDoC to CO.
 - Notify CO of all contract specifications that do not comply with providing full feature functionality for IPv6.
6. **Contracting Officers (CO)**
 - Contracting Officer may rely on the requiring activity's declaration on the APP to determine the applicability of IPv6 requirements to its acquisition. When the APP and the requirements documents provided by the requiring activity establish the applicability of IPv6 in accordance with FAR 11.002, the contracting officer shall:
 - a) Include a contract requirements statement in solicitations that specifically states that products and services that use the Internet Protocol provide full feature functionality in both dual stack (IPv4 and IPv6) and IPv6-only environments in compliance with the NIST USGv6 Testing Program. (See NIST SP 500-267, "A Profile for IPv6 in the U.S. Government – Version 1.0.") The IPv6 requirements statement shall be substantially the same as the statement provided in EPA's contracting writing templates and the IPv6 IT Procurement Checklist; and

- b) Include instructions in solicitations that require offerors to notify the contracting officer of any contract specifications that do not comply with providing full feature functionality for IPv6.

7. Vendors

- Complete and sign an SDoC that specifies and certifies the service or product's IPv6 capabilities and then submit with proposal.

2.3. Waivers

A requestor in an FCC office seeking a waiver to procure an IT product or service that does not meet the IPv6 compliance requirements specified in FAR 11.002(g) and in this policy must submit a signed request via memorandum from the respective Information Official (IO) to the Deputy CIO Office. All IT procurements for hardware, software and services that do not comply with federal and EPA IPv6 requirements require written approval from the CIO.

Per OMB M-21-07, the CIO may issue an IPv6 requirements waiver for an acquisition, if requiring IPv6 would be an undue burden on an acquisition. The waiver must include vendor documentation detailing timelines to incorporate IPv6 capability into the respective product. Waivers will be issued case-by-case only.

Reference Documents

The following external documents provide either governance or guidance for this document.

| Document ID | Document Title |
|-----------------------------|--|
| OMB Memorandum M-05-22 | "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-22.pdf |
| OMB Memorandum (unnumbered) | "Transition to IPv6," September 28, 2010 https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf |
| NIST SP 500-267 | "A Profile for IPv6 in the U.S. Government – Version 1.0," July 2008 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-267.pdf |
| CIO Council | "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government," July 2012 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf |

| Document ID | Document Title |
|--|---|
| NIST website: | “USGv6: A Technical Infrastructure to Assist IPv6 Adoption” https://www-x.antd.nist.gov/usgv6/ |
| FAR Part 11.002(g) | Describing Agency Needs – Policy https://www.acquisition.gov/sites/default/files/current/far/html/Subpart%2011_1.html#wp10%2086792 |
| FAR Part 39 | Acquisition of Information Technology https://www.acquisition.gov/sites/default/files/current/far/html/FARTOCP39.html |
| FCC IT Procurement Check List | Chcklist to be drafted and linked |
| NIST Special Publication 500-267B Revision 1 | https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.500-267Br1.pdf |
| USGv6 Test Methods: General Description and Validation | https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.500-281Br1.pdf |
| USGv6 Test Program Guide | https://www.nist.gov/publications/usgv6-test-program-guide |
| OMB M-21-07 | Completing the Transition to Internet Protocol Version 6 (IPv6), November 2020 https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf |

Appendix A: Definitions

Advanced Procurement Plan (APP): A plan that enables program and procurement officials to identify and schedule procurement requirements in advance of needs.

Dual Stack: Environment in which devices are able to run IPv4 and IPv6 in parallel, allowing hosts to simultaneously reach IPv4 and IPv6 content.

IPv6-Only Capability: A product labeled “IPv6-Only” must support the full lifecycle of operation (including product installation, configuration, operation, management, instrumentation, and update) in environments with no IPv4 capabilities (either not implemented or disabled). A product claiming support of the IPv6-Only capability must be fully functional when deployed in an IPv6-only network. **Note** – The overall concept of IPv6-Only Capability may evolve over time to include all products and services to be operationally IPv6 exclusively.

IPv6-Only Network: IPv6-only can be used only if a complete network, end-to-end, is not natively forwarding IPv4, i.e. IPv4 addresses are not configured for management, nor is the network providing transition/translation support, nor is there IPv4 transit/peering. This includes the following:

- **IPv6-Only WAN/Access** – IPv6-only WAN or access can be used only if the WAN or access network is not actually natively forwarding IPv4.
- **IPv6-only LAN** – IPv6-only LAN(s) can be used only if the LAN(s) is not natively forwarding IPv4.
- **IPv6-only Host/Router** – IPv6-only hosts/routers can be used only if the host/router is not using or forwarding IPv4 (i.e. IPv4 is unconfigured and/or disabled in the external facing interfaces); Internal interfaces such as loopback can still be using IPv4 within the network.

Internet Protocol (IP): A protocol that uses datagrams, or data packets, for sending data through networks. Data are encapsulated in packets that contain routing and identity information so that the network knows where the data comes from and where it is supposed to go. Version 4 is the standard Internet Protocol. IPv6 is being adopted by the federal sector and version 4 will be phased out over time.

Internet Protocol version 6 (IPv6): Internet Protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.

Information Technology (IT): Defined by the Clinger-Cohen Act of 1996, sections 5002, 5141 and 5142, means any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. For purposes of this definition, equipment is "used" by an agency whether the agency uses the equipment directly or it is used by a contractor under a contract with the agency that (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources. It does not include any equipment acquired by a federal contractor incidental to a federal contract.

Supplier's Declaration of Conformity (SDoC): A document which shows that a product, process or service conforms to a standard or technical regulation. The supplier provides written assurance of conformity to the specified requirements. This is also sometimes called Self Declaration of Conformity.

U.S. Government v6 Profile (USGv6): A recommended acquisition guide for IPv6 capabilities in common network products. It is meant as a strategic planning guide for USG IT acquisitions to help ensure the completeness, correctness, interoperability and security of early IPv6 product offerings to protect early USG investments in the technology.