Federal Energy Regulatory Commission

Internet Protocol Version 6 (IPv6) Policy

May 18, 2021

Version 1.0

Federal Energy Regulatory Commission
Cybersecurity and Information Assurance Division
888 1st Street NE
Washington, DC 2042

Document Control

This is a controlled document produced by the Federal Energy Regulatory Commission. The control and release of this document is the responsibility of the document owner. This includes any amendment that may be required.

Document Control	
Date	April 5, 2021
Author	Henrietta Corgie Ahiabenu
Document Title	FERC Internet Protocol Version 6 (IPv6) Policy

Owner Details	
Name	Eric Rippetoe
Office/Region	Federal Energy Regulatory Commission, Washington, DC 20426
Contact Number	(202) 502-6097
E-mail Address	Eric.Rippetoe@ferc.gov

Revision History			
Issue	**Date**	**Author**	**Comments**
0.1	March 19, 2021	Henrietta Corgie-Ahiabenu	Initial Draft
0.2	March 29, 2021	Lemanda Franklin	Reviewed content, updated formatting,
0.3	April 5, 2021	Henrietta Corgie-Ahiabenu	Document Review
1.0	May 18, 2021	Lisa Guevara Escobar	Initial Release

Contents

1. INTRODUCTION

1.1 Authority

Applicable Executive Orders, National Policy, and Public Laws for this policy include the following:

- CIO Council, "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government," July 2012
- Enterprise IPv6 Deployment Guidelines at datatracker.ietf.org
- FAR Part 39 – Acquisition of Information Technology, https://www.acquisition.gov/sites/default/files/current/far/html/FARTOCP39.html
- FAR Part 11.002(g) – *Describing Agency Needs – Policy*
- FAR Part 39 – *Acquisition of Information Technology*
- FAR Part 11.002(g) – *Describing Agency Needs – Policy*
- Federal Acquisitions Regulations (FAR) Part 11.002(g)Federal Information Security Modernization Act of 2014 (FISMA 2014) Public Law 113-283
- IAB Statement on IPv6, The Internet Architecture Board, November 2016
- IPv6 Enterprise Network Scenarios at https://datatracker.ietf.org/doc/rfc4057/
- IPv6 FAR Requirements: Federal Register, Volume 74 Issue 236 (Thursday, December 10, 2009) (govinfo.gov)
- IPv6 Transition/Co-existence Security Considerations at https://datatracker.ietf.org/doc/rfc4942/
- Office of Management and Budget (OMB) memorandum, M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)," dated November 19, 2020
- OMB Circular A-130, "Managing Information as a Strategic Resource"
- OMB Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)," August 2, 2005
- OMB Memorandum (unnumbered), "Transition to IPv6," September 28, 2010
- OMB Circular A-130, "Managing Information as a Strategic Resource"
- Security Considerations at https://datatracker.ietf.org/doc/rfc4942/
- "USGv6 Profile," National Institute of Standards and Technology (NIST) Special Publication 500-267B Revision 1
- "USGv6 Test Program Guide," NIST Special Publication (NIST SP) - 500-281A, Revision 1, November 2020
- "USGv6 Suppliers Declaration of Conformity," NIST Special Publication (NIST SP), 500-281Ar1s, November 2020
- "USGv6 Capabilities Table," NIST Special Publication (NIST SP), 500-267Br1s, November 2020.
- "USGv6 Test Methods: General Description and Validation," NIST Special Publication (NIST SP), 500-281Br1, November 2020

1.2 Purpose

The purpose of this policy is to fully implement the requirement to transition all Federal information systems and services to Internet Protocol Version 6 (IPv6) by the year 2025 as mandated in the Office of Management and Budget (OMB) memorandum, M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)," dated November 19, 2020. This policy is to ensure and enforce the implementation of the Federal Energy Regulatory Commission (FERC) processes in place to assist with the Federal government's strategic commitment to the transition to IPv6 and keep pace with industry trends. To effectively govern and enforce the IPv6 efforts, FERC has established an agency wide IPv6 integrated project team, which includes acquisition, policy, and technical team members. FERC's strategic intent is to phase out the use of Internet Protocol Version 4 (IPv4) for all agency systems. As required by OMB, by Fiscal Year (FY) 2023, all new networked Federal information systems shall be IPv6-enabled at the time of deployment.

1.3 Scope

This policy applies to all FERC information and information systems including those used, managed, or operated by a contractor, another agency, or other organization on behalf of the agency. This policy applies to all FERC employees, contractors, and all other users of FERC information and information systems that support the operation and assets of FERC. Systems under development must meet the System and Communications Protection requirements of FERC's in a manner commensurate with the sensitivity of the information they house and the current life cycle phase. This policy applies to all new FERC's acquisitions of Information Technology (IT) products or services using Internet Protocol (IP), as well as decommissioning existing IPv4 systems.

2. ROLES AND RESPONSIBILITIES

Roles	*Responsibilities*
Executive Director (ED)	• Ensures OMB IPv6 transition compliance and consistency across the agency; and • Provides agency-wide guidance for IPv6 implementation.
Chief Information Officer (CIO)	• Carries out the responsibilities of the Federal Agency CIO as required by Federal law, regulation and policy; • Lead and strategize for cybersecurity infrastructure and operations; • Designates the Chief Information Security Officer (CISO) to carry out the CIO's responsibilities for cybersecurity and IT account management; • Designates the IT Operations Director (ITOps) to operate and maintain the information systems and infrastructure; • Has the authority to set Agency-wide IT policy, including all areas of IT governance such as enterprise architecture and standards, IT capital planning and investment management, IT asset management, IT budgeting and acquisition, IT performance management, risk management, IT workforce management, IT security and operations, and information security; and • Approves or disapproves all IPv6 compliance waivers to this policy.
Chief Information Security Officer (CISO)	• Carries out the Chief Information Officer security responsibilities under Federal Information Security Modernization Act of 2014 (FISMA) and serving as the primary liaison for the Chief Information Officer (CIO) to the organization's Information System Owners, and Information System Security Officers; • Heads an office with the mission and resources to assist the organization in achieving more secure information and information systems in accordance to FISMA requirements; and • Approves all IPv6 upgrades and new purchases.

Roles	*Responsibilities*
Information System Owner (ISO)	• Provides procurement, development, integration, modification, operation, maintenance, and disposal of an information system; • Provides operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements); • Provides the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls; • Responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior); and • Reviews security assessment results from the Security Control Assessor.
Information System Security Officer (ISSO)	• Maintain an inventory of all components of their information system; • Monitor and check for security alerts, advisories, and directives on an ongoing basis for all non-standard components of their information system; • Ensure appropriate prioritization of remediation for non-standard IT resources; • Respond to alerts, advisories, and directives related to components of the information systems by taking appropriate remediation actions within established time frames; • Report any issues associated with application of remediation actions; • Assign individuals to test remediation of information system components; • Train individuals assigned to test information system components as needed; • Maintain distribution lists for alerts, advisories, and directives; • Distribute alerts, advisories, and directives to information system users as appropriate or requested; • Consider carefully the structure and content of error messages that are custom developed for an information system component; • Configure the information system to prevent non-privileged users from circumventing malicious code protection capabilities; and • Configure the information system to prevent non-privileged users from circumventing intrusion detection and prevention capabilities.

Roles	*Responsibilities*
FERC Cybersecurity and Information Assurance Division (CsIA)	• Assist information system owners and managers in carrying out their responsibilities; and • Assist in verifying that remediation actions have been successful.

3. BACKGROUND

OMB Memorandum M-21-07, dated November 19, 2020, outlines the Federal government's strategic intent to deliver its information services, operate its networks, and access the services of others using only IPv6. This memorandum provides Federal agencies with specific requirements for completing the operational deployment of IPv6 across all Federal information systems and services. Serving as a guide for agencies, this memorandum helps agencies identify and overcome obstacles that keep them from migrating to IPv6-only network environments. To keep pace with and leverage the IPv6 progress in networking technology all Federal agencies must move forward with implementing the requirements in memorandum.

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, FERC shall implement the outlined steps provided in OMB Memorandum M-21-07.

4. POLICY

This policy mandates the implementation OMB memorandum, M-21-07, and Federal Acquisitions Regulations (FAR) Part 11.002(g) requirements for all FERC's program office and employees seeking to procure a networked IT product or service, vendors responding to Requests for Proposal (RFP), and acquisition staff involved in the procurement process. The requirements in the OMB M-21-07 also mandate that all existing IPv4 products and services be updated to IPv6, as well as ensure all new acquisitions of IT products or services are IPv6 compliant. The Agency is actively implementing these policy updates to ensure IPv6 requirements are in place and align with the overall goal 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 Federal government is capable of accessing IPv6-only services.

FERC shall actively implement the following:

- All new networked Federal information systems to be IPv6-enabled at the time of deployment to ensure the IPv6 only requirement is met no later than FY 2023. It is the agency's strategic intent to phase out the use of IPv4 for all systems.
- Shall work to identify opportunities for IPv6 pilots and shall 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.
- Shall develop an IPv6 implementation plan by the end of FY 2021 and update the Information Resources Management (IRM) Strategic Plan as appropriate, to update all networked Federal information systems (and the IP-enabled assets associated with these systems) to fully enable native IPv6 operation.

The IPv6 implementation 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; and
- At least 80% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2025.

FERC shall:

- Identify and justify Federal information systems with their agency that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems.
- Shall 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.
- Shall complete the upgrade of public/external facing servers and services (e.g., web, email, Domain Name System (DNS), and Intrusion Prevention System (ISP) services) and internal client applications that communicate with public Internet services and supporting enterprise networks to operationally use native IPv6.

5. POLICY COMPLIANCE

To comply with OMB-M-21-07, FERC must enforce and implement the federal requirement outlined in this policy. Only FERC's CIO or a designee shall approve or disapprove all IPv6 compliance waivers to this policy. The 2010 memorandum requires 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 upgrade both in future agency IPv6 transition plans and reports:

- Public and/or external facing servers and services (e.g., web, email, DNS, ISP services, etc.) to operationally use native IPv6; and
- Internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6.

6. ADHERING TO FEDERAL IPv6 ACQUISITION POLICY REQUIREMENTS

FERC shall ensure that future acquisitions of networked information technology include IPv6 requirements as mandated in FAR Council amendment issued in December 2009. Unless the FERC's CIO or designee waives the requirement, the Agency acquiring information technology using Internet Protocol shall develop requirements documents to include reference to the appropriate technical capabilities defined in the U.S. Government Version 6 (USGv6) Profile, National Institute of Standards and Technology (NIST Special Publication (SP) 500-267 and the corresponding declarations of conformance defined in the USGv6 Test Program. The FERC acquisition approach shall enable natural technology refresh cycles to upgrade the installed base of networked IT products and services to be IPv6-capable. The Executive Director shall ensure that Federal IT systems are positioned to leverage the technical and economic benefits of IPv6, and eventually migrate to IPv6-only environments when appropriate.

In accordance with existing FAR requirements, FERC shall:

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

A requestor in FERC office seeking to procure an IT product or service using IP must work with their Contracting Officer (CO) to ensure appropriate IPv6 requirements language is included in the following documents:

- Procurement Requests (PR),
- Advanced Procurement Plans (APP),
- Statements of Work (SOW),
- Requests for Proposal, and
- Awarded Contracts

7. EVOLVING THE USGv6 PROGRAM POLICY REQUIREMENTS

NIST will continue to update and expand the USGv6 Program and provide periodic updates to the USGv6 Profile to incorporate the latest Internet Engineering Task Force (IETF) specifications relevant to IPv6 technology. FERC shall continue to monitor updates from the USGv6 Program to ensure the agency maintains consistency with IPv6 changes of other government agencies, as well as continue to monitor and adhere to updates from NIST as required per FISMA. FERC shall enforce the following policy requirements:

- Avoid any unnecessary duplication of generic testing requirements by leveraging the USGv6 Test Program for basic conformance and general interoperability testing of commercial products.
- Ensure that the agency or acquisition specific testing focus on specific systems integration, performance, and information assurance testing not covered in the USGv6 Test Program.

8. ENSURING ADEQUATE SECURITY

To help ensure the security benefits of IPv6 for all Federal agencies, the FERC shall require the following requirements are in place for all FERC's information systems:

- Include plans for full support of production IPv6 services in IT security plans, architectures, and acquisitions;
- Validate 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;
- Follow applicable Federal guidance and leverage industry best practices, as appropriate, for the secure deployment and operation of IPv6 networks; and
- Ensure that all security and privacy policy assessment, authorization and monitoring processes fully address the production use of IPv6 in Federal information systems.

9. PRODUCT AND SERVICE PROCURES REQUESTS

The following are the requirements for FERC staff to follow in order to request procurement of IT products and services:

- Include appropriate IPv6 requirements language in PR and APP;
- Work with CO to ensure appropriate IPv6 requirements language is included in Statements of Work (SOW), 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 Supplier's Declaration of Conformity (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; and
- Notify CO of all contract specifications that do not comply with providing full feature functionality for IPv6.

10. CONTRACTING OFFICERS

The FERC CO shall review APP to determine the applicability of IPv6 requirements to its acquisition. The CO shall ensure the APP and supporting documents are in accordance with FAR 11.002(g) IPv6 requirements by including:

- 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.
- Contract requirements statement in solicitations that specifically states that products and services that use Internet Protocol provide full feature functionality in IPv6-only environments in compliance with the NIST USGv6 Testing Program.
- The IPv6 requirements statement shall be substantially the same as the statement provided in FERC's contracting writing templates and the IPv6 IT Procurement Checklist.

11. VENDORS

Vendors shall complete and sign a Supplier's Declaration of Conformity (SDoC) that specifies and certifies the product's IPv6 capabilities to submit with the proposal.

12. WAIVERS

Only the FERC's CIO or a designee may waive the IPv6 requirements and must do so in writing. A requestor within the FERC seeking a waiver to retain an IT product or service that does not meet the IPv6 compliance requirements specified in OMB-M-21-07, FAR 11.002(g), and in this policy must submit a signed request in memorandum format to the FERC'S CIO. All IT hardware, software and services that do not comply with Federal and FERC IPv6 requirements require written and signed approval from the CIO.

13. APPENDIX A: ACRONYMS

Acronym	*Definition*
APP	Advanced Procurement Plans
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CO	Contracting Officer
CsIA	Cybersecurity Information Assurance Division
DNS	Domain Name Service
FAR	Federal Acquisition Regulations
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version
IoT	Internet of Things
IRM	Information Resources Management
ISO	Information System Owner
ISP	Intrusion Prevention System
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PR	Procurement Requests
RFP	Requests for Proposal
SP	Special Publication
SOW	Statements of Work
SDoC	Supplies Declaration of Conformity
USG	U.S. Government
USGv6	U.S. Government v6 Profile