Federal Energy Regulatory Commission

Internet Protocol Version 6 (IPv6) Policy

January 29, 2026

Federal Energy Regulatory Commission
Cybersecurity and Information Assurance Division
888 1st Street NE
Washington, DC 20426

Document Control

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

Table 1. Owner Details

Name	Amir Dastouri
Office/Region	Federal Energy Regulatory Commission, Washington, DC 20426
Contact Number	(202) 502-8224
E-mail Address	Amir.Dastouri@ferc.gov

Table 2. 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
0.3	April 5, 2021	Henrietta Corgie-Ahiabenu	• Document Review
1.0	May 18, 2021	Lisa Guevara Escobar	• Initial Release
1.1	June 13, 2023	Lemanda Franklin	• Completed biennial review • Updated document to be 508 compliant • Updated all sections based on meeting with IPv6 Team. Also, removed references to specific dates, which will be moved into the IPv6 Detailed Implementation Plan.
1.2	June 20, 2023	Michael Martone	• Reviewed document and made updates to Section 4.0 to add general phased approach content. • Approved removing dates from document and will place dates and % completion information into the IPv6 Detailed Implementation Plan.
1.3	October 18, 2023	Lemanda Franklin	• Reviewed updates to document. • Updated the Authority section of document.

Issue	Date	Author	Comments
2.0	November 27, 2023	Lemanda Franklin	• Updated document per comments for each section of the document. • Removed the Background section to be in line with formatting/layout of other policies.
3.0	February 01, 2024	Lemanda Franklin, Lisa Weber	• Updated policy.
4.0	October 29, 2025	Lemanda Franklin, Lisa Weber, Chalonda Curtis, Dennis Grey, and Vijay Vakkalanka	• Biennial Review

Table of Contents

1.0 INTRODUCTION 5
1.1 Authority 5
1.2 Purpose 5
1.3 Scope 6
2.0 ROLES AND RESPONSIBILITIES 6
3.0 POLICY 7
4.0 POLICY COMPLIANCE 8
5.0 ADHERING TO FEDERAL IPv6 ACQUISITION POLICY REQUIREMENTS 8
5.1 PRODUCT AND SERVICE PROCUREMENT REQUESTS 9
6.0 EVOLVING THE USGv6 PROGRAM POLICY REQUIREMENTS 9
7.0 ENSURING ADEQUATE SECURITY 10
8.0 CONTRACTING OFFICERS 10
9.0 VENDORS 10
10.0 WAIVERS 10
11.0 APPENDIX A: ACRONYMS 11
12.0 APPENDIX B: APPROVAL 12

List of Tables

Table 1. Owner Details 2
Table 2. Revision History 2
Table 3. Roles and Responsibilities 6
Table 4. Acronyms 11

1.0 INTRODUCTION

1.1 Authority

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

- CIO Council, *Planning Guide/Roadmap Toward Internet Protocol Version 6 (IPv6) Adoption within the U.S. Government*
- Enterprise IPv6 Deployment Guidelines at datatracker.ietf.org
- Federal Acquisitions Regulations (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
- Federal Information Security Modernization Act of 2014 (FISMA 2014) Public Law 113-283
- IAB Statement on IPv6, The Internet Architecture Board
- IPv6 Enterprise Network Scenarios at https://datatracker.ietf.org/doc/rfc4057/
- IPv6 FAR Requirements: Federal Register, Volume 74 Issue 236, https://www.govinfo.gov/content/pkg/FR-2009-12-10/pdf/E9-28931.pdf
- 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 IPv6*
- OMB Circular A-130, *Managing Information as a Strategic Resource*
- OMB Memorandum M-05-22, *Transition Planning for IPv6*
- OMB Memorandum, M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*
- OMB Memorandum (unnumbered), *Transition to IPv6*
- OMB Circular A-130, *Managing Information as a Strategic Resource*
- Security Considerations at https://datatracker.ietf.org/doc/rfc4942/
- National Institute of Standards and Technology (NIST) Special Publication (SP) 500-267B, Revision 1, *USGv6 Profile*
- NIST SP 500-281A, Revision 1, *USGv6 Test Program Guide*
- NIST SP 500-281Ar1s*USGv6, USGV6 Suppliers Declaration of Conformity*
- NIST SP 500-267Br1, *USGv6 Capabilities Table*
- NIST SP 500-267B, Revision 1, *USGv6 Profile*
- NIST SP500-281Br1, *USGv6 Test Methods: General Description and Validation*

1.2 Purpose

The purpose of this policy is to establish how FERC will govern and implement IPv6 to ensure and enforce FERC's strategic commitment to 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.

FERC shall follow OMB Memorandum M-21-07, which provides the mandates for the Federal government's strategic intent to deliver its information services, operate its networks, and access the services of others using only IPv6. IPv6 growth will continue to accelerate as information technology continues to evolve toward mobile platforms, Internet of Things (IoT), and wireless networks. 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 M-21-07.

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 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 acquisitions of Information Technology (IT) products or services using Internet Protocol (IP), as well as decommissioning existing IPv4 systems.

2.0 ROLES AND RESPONSIBILITIES

Table 3. Roles and Responsibilities

Roles	Responsibilities
Chief Information Officer (CIO)	• Ensures OMB IPv6 transition compliance and consistency across the FERC; • Provides FERC-wide guidance for IPv6 implementation; • Carries out the responsibilities of the Federal Agency CIO as required by Federal law, regulation, and policy; • Leads and strategizes 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 with FISMA requirements; and • Approves all security aspects of the 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.
Cybersecurity and Information Assurance (CsIA)	• Provides hardening and configurations for IPv6 devices; • Accredits network environment as part of the General Support System (GSS); • Monitors network activities on IPv6; and • Assists in verifying that remediation actions have been successful.
IT Operations (ITOps)	• Operations and Maintenance of FERC network equipment and configurations; • Responsible for inventory tracking and validation; • Manages vendor relationships and support/maintenance process; • Provides planning and management of IPv6 projects; • Creates IPv6 design, architecture, and mapping of IPv4 to Ipv6 addresses; • Configure network routing to correctly route both IPv4 and IPv6 addresses; • Coordinate with FERC vendors for IPv6 updates and considerations; • Execute IPv6 Network and Infrastructure changes, IPv6-only and dual-stack actions, across network; and • Testing traffic flows and custom application functions.

3.0 POLICY

This policy mandates the implementation OMB Memorandum, M-21-07, and Federal Acquisitions Regulations (FAR) Part 11.002(g) requirements for all of FERC's program office and employees seeking to procure a networked IT product or service and acquisition staff involved in the procurement process. The FERC 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, and ensure the Federal government is capable of accessing IPv6-only services.

FERC shall actively implement the following, according to the timeline documented in the FERC IPv6 Detailed Implementation Plan:

- Ensure all new networked Federal information systems are IPv6-enabled at the time of deployment to ensure the IPv6 only requirement is met. It is the agency's strategic intent to phase out the use of IPv4 for all systems. FERC requires that all IPv4 systems be upgraded to IPv6 upon the next acquisition cycle.
- Continue to identify opportunities for IPv6 pilots, complete at least one pilot of an IPv6-only operational system and report the results of the pilot to OMB upon request.
- Maintain and update the F*ERC IPv6 Implementation Plan and Strategic Information Resources Management (IRM) Plan* as appropriate, update all networked Federal information systems (and the IP-enabled assets associated with these systems) to fully enable native IPv6 operation.

The FERC IPv6 Detailed Implementation Plan shall provide the FERC's transition process and include the milestones and actions to ensure IP-enabled assets on FERC's network are operating in the IPv6-only environment and meet the determined percentages by the dates designated in the FERC IPv6 Detailed Implementation Plan. FERC shall also continue to make progress to dual stack and work toward the goals documented in the FERC IPv6 Detailed Implementation Plan according to the below general phased approach:

- Enable Dual-Stack on the Network Infrastructure;
- Build DNS6 and DHCP6 supporting capabilities;
- Enable End-point Dual-Stack; and
- Enable Native IPv6.

FERC shall:

- Identify and justify Federal information systems within FERC that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems.
- 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.
- Complete the upgrade of public and/or 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.

4.0 POLICY COMPLIANCE

Only FERC's CIO or a designee shall approve or disapprove all IPv6 compliance waivers to this policy.

The FERC shall ensure the following operationally use native IPv6:

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

5.0 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, upon acquisition of any information technology using Internet Protocol, the FERC shall develop requirement documents that include reference to the appropriate technical capabilities defined in the U.S. Government Version 6 (USGv6) Profile, NIST 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 CIO 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;
- Include IPv6 requirements into all future procurements.
- Continue to require potential vendors to document compliance with such IPv6 requirement statements through the USGv6 Test Program; and
- Provide a process for FERC's CIO to waive this requirement on a case-by-case basis such as in rare circumstances where the requirement demonstrates that IPv6 capabilities would pose undue burden on an acquisition action. In such cases, the purchasing agency shall request documentation from vendors detailing explicit plans (e.g., timelines) to incorporate IPv6 capabilities into their offerings.

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

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

5.1 PRODUCT AND SERVICE PROCUREMENT 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 Procurement Requests and Advanced Procurement Plans;
- Work with CO to ensure appropriate IPv6 requirements language is included in Statements of Work (SOW), RFPs and awarded contracts; and
- Analyze that the vendor meets FERC requirements and complies with Federal guidance.

6.0 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; and

- Ensure that the agency or acquisition specific testing focuses on specific systems integration, performance, and information assurance testing not covered in the USGv6 Test Program.

7.0 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 of FERC's information systems in addition to all existing FERC polices:

- Include plans for full support of production IPv6 services in IT security plans, architecture, 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.

8.0 CONTRACTING OFFICERS

The FERC CO shall review advanced procurement plans 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 requirement statements in solicitations shall specifically state that products and services that use Internet Protocol provide full feature functionality in IPv6-only environments in compliance with the NIST USGv6 Testing Program.

9.0 VENDORS

All vendors shall complete and meet the requirements of *Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Secure Software Development Attestation Form*. As documented in both the *FERC Supply Chain Risk Management Policy* and *FERC Supply Chain Risk Management Strategy* document, vendors shall be further evaluated to determine if the vendor already meets the government-wide attestation requirement or if FERC needs to provide the DHS Self-Attestation Form to the vendor for completion.

10.0 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 Memorandum 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.

11.0 APPENDIX A: ACRONYMS

Table 4. Acronyms

Acronym	Definition
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
RFP	Requests for Proposal
SP	Special Publication
SOW	Statements of Work
USG	U.S. Government
USGv6	U.S. Government v6 Profile

12.0 APPENDIX B: APPROVAL

I hereby approve the implementation of this Internet Protocol Version 6 (IPV6) Policy. This Policy will become effective upon signature.

Signature: AMIR DASTOURI Digitally signed by AMIR DASTOURI Date: 2026.01.30 07:25:38 -05'00' Date: _____

Amir Dastouri
Chief Information Security Officer (CISO)

Signature: MITTAL DESAI Digitally signed by MITTAL DESAI Date: 2026.01.30 08:34:13 -05'00' Date: _____

Mittal Desai
Chief Information Officer (CIO)