FCC INFORMATION TECHNOLOGY (IT) IPv6 IMPLEMENTATION PLAN

OFFICE OF THE MANAGING DIRECTOR
45 L Street NE, Washington, DC 20002

Record of Approval

Document Approval	
<Document POC>	
Printed Name: Associate CIO – Data & Policy	
Signature: Arecio Dilone Digitally signed by Arecio Dilone Date: 2021.10.07 12:22:17 -04'00'	**Date:**
<Approval Structure>	
Printed Name: Chief Information Officer	
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: 2021.10.12 09:39:18 -04'00'	**Date:**
Printed Name: Deputy CIO – Management & Lifecycle	
Signature: Jennifer H. Bilbrey Digitally signed by Jennifer H. Bilbrey Date: 2021.10.07 14:18:55 -04'00'	**Date:**
Printed Name: Deputy CIO – Technology Execution	
Signature: Shaun H. Costello - DCIO Digitally signed by Shaun H. Costello - DCIO Date: 2021.10.08 08:22:51 -04'00'	**Date:**
Printed Name: Chief Information Security Officer	
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: 2021.10.07 12:43:40 -04'00'	**Date:**

Revision Log

Date	Description	Author
October 6, 2021	First Draft for publishing to FCC.gov	Project Team

Table of Contents

List of Tables

1. Introduction

FCC IT Data & Policy team will take the lead on coordinating the implementation, operational deployment, and use of Internet Protocol version 6 (IPv6) for the FCC. IPv6 is the next-generation Internet protocol, designed to replace version 4 (1Pv4) which has been in use since 1983.

OMB Memorandum M-21-07 instructs the Federal Government to deliver its information services, operate its networks, and access the services of other agencies networks using only IPv6.

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.

As information technology continues to evolve toward mobile platforms, Internet of Things (IoT), and wireless networks, IPv6 growth will continue to accelerate.

FCC IT Data & Policy will coordinate with relevant POCs/Owners on respective utilization/confirmation of use for the next three-to-five years, operation, deployment, and handoff.

1.1 Program Overview and Objectives

The goal of the FCC's IPv6 Implementation is to bring the agency into compliance with OMB Memorandum M-21-07, which mandates federal agencies to deliver its information services, operate its networks, and access external non-governmental internet resources using only IPv6.

1. Designate an agency wide IPv6 integrated project team (including acquisition, policy, and technical members), or other governance structure, within 45 days of issuance of this policy 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 Fiscal Year (FY) 2023, all new networked federal information systems are IPv6-enabled at the time of deployment, and state the agency's strategic intent to phase out the use of IPv4 for all 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 0MB upon request
   - *FY21 Status – Due to IT staffing and contract transitions, the IPv6 Pilot is in its initiating stage. The Pilot recommendations in this section reflect initial research and planning. FCC IT approval, prioritization, and funding are pending. The Project Team will confirm and refine Pilot information during project progression, and will publish Pilot results upon completion.*
4. 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 plan shall describe the agency transition process and include the following milestones and actions:
   a. At least 20% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2023

   b. At least 50% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2024
   c. At least 80% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2025
   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 and develop plans to migrate all such network interfaces to the use of IPv6
6. Complete the upgrade of public/external facing servers and services (*e.g.,* web, email, DNS, and ISP services) and internal client applications that communicate with public Internet services and supporting enterprise networks to operationally use native I249-Pv6
7. Ensure that plans for full support for production IPv6 services are included in IT security plans, architectures, and acquisitions
8. Ensure that all systems that support n4etwork 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
9. Follow applicable Federal guidance and leverage industry best practices, as appropriate, for the secure deployment and operation of IPv6 networks
10. Ensure that all security and privacy policy assessment, authorization and monitoring processes fully address the production use of IPv6 in Federal information systems

1.2 Program Organization, Roles, and Responsibilities

1.2.1 Key Resources

Table 1. Key Resources

IPT Member	Role
Chief Information Officer	Sponsor
DCIO of Management & Lifecycle	Business Lead
DCIO of Technology Execution	Business Lead
Lead IT Specialist – Enterprise Engineering & Architecture	Technical Lead
ACIO – Data & IT Policy	Project Lead
ACIO – Applications Development and Support	IPT Member
Cybersecurity Engineering Lead	IPT Member
ACIO – Enterprise IT Operations and Services	IPT Member
Information Resource Manager, Budget & Acquisitions Team	IPT Member

Contract Senior Project Manager	Highlight Technologies

Table 2. FCC IT Key Resources

FCC IT Member Name	Role
ACIO – Stakeholder Relations	IPT Member
ACIO – Enterprise Planning & Performance	IPT Member

Table 3. OMD Stakeholders

OMD Member Name	Role
OMD Front Office	Managing Director
OMD Front Office	Deputy Managing Director
OMD Front Office	Deputy Managing Director

Additional resources may be identified as the IPv6 Implementation program and sub projects progress.

1.2.2 Major Tasks & Implementation Schedule

Dates will be inputted during program/sub-project progression.

Table 4. Major Tasks

Task Description	Owner	Implementation Schedule/Due Date
Train network technical staff	Engineering Operations & Services	TBD
Check all required security, management, operational and accounting tools for IPv6 capability	Enterprise Operations & Services, Enterprise Engineering & Architecture, Applications Development & Support, Cyber Security	TBD
Determine the type of IPv6 address space needed	Enterprise Engineering & Architecture	TBD
Determine the amount of space needed	Enterprise Engineering & Architecture	TBD
Design an addressing plan (with potential redesigns)	Enterprise Engineering & Architecture	TBD
Audit all network hardware for IPv6 capabilities including firewall and/or intrusion detection/prevention equipment	Enterprise Operations & Services, Enterprise Engineering & Architecture, Applications Development & Support, Cyber Security	TBD
Establish IPv6 connectivity with network provider(s)	Enterprise Engineering & Architecture, Applications Development & Support	TBD

Task Description	Owner	Implementation Schedule/Due Date
Decide on use of State Less Address Auto Configuration (SLAAC)	Enterprise Engineering & Architecture	TBD
Test connectivity to external systems	Enterprise Engineering & Architecture	TBD
Enable IPv6 for DNS	Enterprise Engineering & Architecture	TBD
Enable IPv6 for other services	Enterprise Engineering & Architecture	TBD

2. Scope of this Document

The scope of this document is to define and establish processes and procedures for the effective planning for the implementation of IPv6 with a goal of meeting the requirements of the OMB M-21-07.

3. Assumptions, and Risks

3.1 Assumptions

- All milestones will need to be prioritized, projectized separately, funded, and staffed to make OMB deadlines
- No funding allocated for the immediate future (including FY21 and FY22)
- Technical ACIOs will be resource-constrained in terms of staffing and funding
- The CIO and OMD will need to compel stakeholder cooperation

3.2 Risks

Table 5. Enterprise Level Risks

Status	Description	Mitigation	Likelihood	Impact
Open	Stakeholder Engagement – If stakeholders do not actively participate with the Project Team, then key tasks may slip, pushing back timelines.	The PM will monitor and appraise the Business Lead and Sponsor of potential gaps in meeting commitments and engagement and recommend corrective actions.	H/M/L	H/M/L
Open	Procurement Timelines – If procurement of necessary resources and services is held up through additional decision-making steps, then timelines within the OMB-directed deadlines may slip.	The PM will monitor and appraise the Project Team of potential Schedule impact, and recommend corrective actions.	H/M/L	H/M/L
Open	Leadership Intervention – If IT (and potentially OMD) Leadership does not compel cooperation from stakeholders, then achieving OMB-ordered milestones will be missed, pushing back timelines.	The ACIO-D&P will recommend CIO direction and orders to the IPT Members.	H/M/L	H/M/L
Open	Staffing Transitions – If IT is unable to replace departed staff members, then gaps in key positions (including Engineering and Enterprise Architecture) may lead to timeline slippage and failure to make OMB milestones.	The ACIO-D&P and Senior PM will monitor	H/M/L	H/M/L

4. Implementation Schedule

The IPv6 Implementation Project Team will deliver a weekly MS Project IMS to the PMO and Enterprise Performance & Planning (EPP).

The IPv6 Implementation Project Schedule is located in the FCC IT PMO's SharePoint folder.

5. Implementation

Implementation will cover the following areas:

- Transition Planning and Analysis
  - Training
  - Network Infrastructure Assessment and IPv6 Impact (i.e. Inventory) - All Technical and Security IPT members
  - IPv6 Addressing Plan and Network Architecture (for Engineering and Operations)
  - IPv6 Deployment Strategy
- IPv6 Test and Integration
  - Set up the Test Lab
  - Test Integration in the Test Lab
- Pilot Production Deployment on Selected LANs
- IPv6 Deployment to Production

5.1 Transition Planning and Analysis

The IPv6 transition planning shall ensure that network, computing, application, and service components are enabled in a sequence that maximizes the benefit to the Agency's business mission through meaningful end-to-end IPv6 activity. FCC IT expects that each target milestone will require IT and OMD Leadership prioritization, projectization, funding, and staffing to make OMB-directed milestones.

5.1.1 Training

IPv6 Training for appropriate Agency personnel involved with the Agency network infrastructure shall include identifying initial and ongoing IPv6 training requirements for FCC IT review, comment, and approval. At a minimum, training shall describe the schedule, curriculum, materials, and the resources required to ensure that the IPv6 training meets the FCC's needs. Training types shall include the following:

- Security staff to understand and mitigate the risks of IPv6 transition
- Network architects on how to take full advantage of IPv6 capabilities
- Application developers on how to use IPv6 features and capabilities to improve the Agency's network security services
- IT employees who are involved with the network or desktop management, including employees on operations teams, to understand how IPv6 affects their areas of responsibility

5.1.2 Network Infrastructure Assessment and IPv6 Impact - All Technical and Security IPT Members

The Network Infrastructure Assessment / IPv6 Impact Analysis shall describe all activities related to discovery of the Agency infrastructure and the network, server, and application elements to be assessed. This includes the following:

- Creation of a detailed assessment of FCC IT services, equipment, and applications impacted by IPv6 based on information provided by the FCC, or preferably via an automated tool (network analyzer, packet capture, protocol analyzer). Protocol analysis shall include all Layer 2 and Layer 3 protocols, including legacy protocols such as SNA and DECnet that transit each segment of the Agency network. The items to be assessed include but are not limited to:
    - Networked Devices: Data Center Servers, Client Access (PCs), Printers, Collaboration Devices and Gateways, Sensors and Controllers
    - Network Infrastructure: DNS and DHCP, Load Balancing and Content Switching, Security (Firewalls, and IDS/IPS), Content Distribution, Optimization (WAAS, SSL Acceleration), and VPN Access
    - Web applications
    - Applications and application suites
- Assessment of FCC IT services, equipment, and applications that needs to be upgraded, replaced, or enabled for IPv6. Each version shall be analyzed and assigned to one of the following categories:
    - Currently running IPv6
    - IPv6-compliant but device needs to be configured for IPv6
    - Requires software upgrade for IPv6 compliance
    - Requires hardware upgrade to support software upgrade
    - Legacy platform: cannot be upgraded to support IPv6 and must be replaced
    - Will not be upgraded due to planned discontinuation

FCC IT will leverage services for initial inventory tracking, and recommends the following to facilitate:

- Implement ServiceNow Discovery and CMDB to discover and track device and technology level data
- Implement Dynatrace to automate and maintain application mapping and integrate into ServiceNow CMDB
- Validate application inventory (Ardoq, AWS)
- Validate TRM with ServiceNow discovery, LiquidWare StratuSphere, and SCCM data

5.1.3 IPv6 Addressing Plan and Network Architecture (for Engineering and Operations Groups)

FCC IPv6 Address Assignment

FCC has a direct assignment for IPv6 address space from ARIN, assigned on May 9th, 2007 – 2620:0:610::/44. This is the equivalent to FCC's 165.135.0.0/16 IPv4 address space used for internal network at FCC. This block of IPv4 address space is directly assigned from ARIN to FCC and does not change. FCC is also using RFC1918 Private Internet Addresses – 172.16.0.0/16 and 10.0.0.0/8.

The RDF1918 addresses, and specifically the 10.0.0.0/8 address space, are used for most of the network and WAN for the FCC. These addresses are not reachable from the Internet (called non-routable IP addresses), so security is improved by FCC workstations not being directly reachable from external networks and IP traffic is only allowed outbound after a Network Address Translation on the DMZ firewalls.

The IPv6 address space of /44 gives FCC 2^20 (1,048,576) potential networks each with 2^64 (1.84e19) hosts.

IPv6 Addressing Background

An IPv6 address is 128 bits versus and IPv4 address having 32 bits. IPv6 does not support broadcast addresses, but instead uses multicast addresses for broadcast. In addition, IPv6 defines a new type of address called anycast. Where IPv4 is represented in decimal quads (165.135.241.15) IPv6 is represented as 8 groups of 16 bits in hexadecimal notation (2620:0000:0610:0001:0200:F8FF:FE75:50DF). Leading zeros are omitted, and a group of zeros are replaced with ":" (once) such as 2620::610:1:200:F8FF:FE75:50DF. The first 64 bits is considered the network portion and the second 64 bits the host portion. In IPv4 an end-user device normally has one IP address. With IPv6, multiple addresses are active at any time.

IPv6 Anycast

Anycast is a network addressing and routing methodology in which a single destination IP address has multiple routing paths to two (or more) endpoint destinations. Routers will determine the desired path based on the number of hops, distance, lowest cost, latency measurements, or the least congested route. Anycast networks are widely used for content delivery network (CDN) products to bring their content closer to the end-user.

Link Local

Link Local IPv6 addresses are meant to be used inside an internal network and are not routed on the Internet. It is equivalent to the IPv4 address 169.254.0.0/16, which is allocated on an IPv4 network when no DHCP server is found.

Link local addresses start with fe80; they are restricted to a link and are not routed on the internal network or the Internet.

Unique Local

Unique Local IPv6 addresses are meant to be used inside an internal network. They are routed on the internal network but not routed on the Internet. They are equivalent to the IPv4 addresses 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. The address space is divided into two /8 spaces: fc00::/8 for globally assigned addressing, and fd00::/8 for locally assigned addressing.

Loop Back

The IPv6 loopback address is ::1. It can be pinged as follows with the ping ::1 command.

SLAAC

Stateless Address Auto-Configuration (SLAAC) is one method of assigning IPv6 address to a given host. SLAAC is stateless (does not require a server and communications to assign an IPv6 address) and builds the IPv6 address by:

- Listening for Router Advertisements (RA) for the network address
- Using the host's MAC address with "FF:FE" injected in the middle for the host address
- The MAC is 48 bits; the 24 high order bits is the vendor code and 24 low order bits are the host portion. The resulting IPv6 host address is [vendor code]FF:FE[Host]. In addition, the MAC address is guaranteed to be unique; no address collision is possible.

IPv6 Reservation

As the address space assigned to the FCC is sufficiently large (/44), IT recommends to reserve 3/4 of the address space for future use. FCC will reserve any network address with high order bits of 00, 01, and 10. This will result in 262,144 potential networks for initial IPv6 deployment.

Subnet Block Sizes

The block sizes need to be determined in an addressing plan and the blocks need to be sufficiently large to handle future growth and technology changes. At maximum, 10% of the possible allocations on any block should be utilized, leaving 90% for future use.

With IPv4, it is common to use /30 or /31 for point-to-point links and interconnects due to address space conservation. With IPv6, this is no longer necessary. For simplicity, the FCC should leverage /64 address blocks for this purpose.

Current recommended block sizes:

- Data Center Locations (Building/Campus) - /48 (for oNoMa, ABL, GB)
- Enterprise functions - /50 (for Perimeter NAT)
- Field locations - /50
- Host subnets - /64
- Interconnects - /64
- Point-to-Point links - /64

Routing Table

In order to keep the IPv6 routing tables as organized and short as possible, a hierarchical addressing scheme must be leveraged. The hierarchical scheme will require that all IP ranges leveraged for a given location are

contained within a given address block. This way, the global routing table will have a single entry for all routing to that location. This is equivalent to route summarization or supernetting in IPv4.

The FCC's deployment of IPv4 is leveraging multiple address blocks per location as a result of shortage of IPs and not having sufficient unallocated addresses in the initial IP deployment, which complicates routing tables and adds complexity to the network. With the sufficient address space of FCC's IPv6 allocation, this issue can be avoided, and a hierarchical address implementation maintained.

5.1.4 IPv6 Deployment Overview

The FCC shall develop an IPv6 Deployment Strategy that lists services, hardware, and software to be purchased and describes how it will be upgraded to IPv6 and made operational in the production network. More specifically, the FCC shall:

- Develop deployment strategies to integrate IPv6 into the network infrastructure:
  1. The IPv6 deployment strategy shall support the following objectives:
     - Avoid any disruption to the delivery of mission-critical Government services over the existing network. This includes current IPv4 capabilities, performance, security, and integration with all network management
     - Identify when an Agency does not own or have available the source code of older applications and intends to upgrade them to IPv6
     - Identify when it makes sense to wait to replace older operating systems or platforms until their end of life
     - Maintain the Agency's security posture throughout the deployment
     - All Agency systems, software, and equipment, or their replacements, shall be supported by IPv6 in an equivalent or better way than current IPv4 capabilities, performance, and security.
  2. IPv6 transition mechanisms for FCC applications shall be developed for:
     - Dual IPv4/IPv6 stack (Note: when the Agency WAN is based on the Networx contract, e.g., NBIP-VPNS, it is already dual IPv4/IPv6 stack capable)
     - IPv6 over MPLS backbone (Note: The Networx backbone is based on IP over MPLS over SONET)
     - IPv6 over IPv4 tunnels
- The FCC shall select appropriate IPv6 requirements including IPv6 features and capabilities that the Agency needs, which are defined in an IETF Request for Comment (RFC) or other well-known reference, such as the IPv6 Special Interoperability Certification from the Defense Information System Agency (DISA) in accordance with the Department of Defense IPv6 Master Test Plan, and the latest guidance on the National Institute of Standards and Technology (NIST) and optionally the Joint Interoperability Test Command (JITC).
- The FCC shall develop an IPv6 Upgrade Plan for upgrading existing software, services, and monitoring tools:

1. For each host on the network, the FCC shall identify its operating system and applications to determine if hardware and software upgrades are required
2. The FCC shall identify one or more applications to be tested in the IPv6 Test Lab

- The FCC shall draft an exception strategy to Identify applications or systems that will likely not be modified in the foreseeable future (nearing end of life) and will continue to use Network Address Translation / Protocol Translation (NAT/PT).
- The FCC shall create and develop a document that defines the baseline for the Agency's IPv6 transition, organized to permit testing and assess completeness

5.2 IPv6 Pilot Test and Integration

FY21 Status – Due to IT staffing and contract transitions, the IPv6 Pilot is in its initiating stage. The Pilot recommendations in this section reflect initial research and planning. FCC IT approval, prioritization, and funding are pending. The Project Team will confirm and refine this section during progression, and will publish Pilot results upon completion.

The test environment should resemble the production environment as closely as possible, including the network hardware and software features targeted for IPv6 integration, as well as the first applications scheduled to operate over IPv6. Initially, the test sites should not be connected to the production network or to each other. Once successful testing has been completed, such connections can be prudently made. The FCC may use a virtualized (software-based) Test Lab and environment if doing so is more cost-effective. IPv6 Test and Integration includes the following testing progression:

1. Set up a Test Lab modeled on the Agency's network infrastructure
2. Test IPv6 integration for network infrastructure and applications in the Test Lab against the IPv6 Transition Baseline document developed in the previous task

5.2.1 Test Lab Setup

The FCC shall establish an IPv6 Test Lab to test changes before they are deployed in the production environment:

- Establish automated network configuration and inventory management for IPv4 and IPv6 to minimize the risk of human error during testing and transition
- Set up the test environment to resemble the production environment as closely as possible, including the network hardware and software targeted for IPv6 transition, as well as the first applications that will operate over IPv6
- Set up routers and switches to process IPv6 traffic, and configure the LAN for its ability to transport the FCC's IPv6 prefixes to production host computers, printers, and other devices
- Ensure that the security architecture is integrated with the overall FCC enterprise architecture and is configured to handle both IPv4 and IPv6, and set up the DNS and DHCP servers to handle IPv6 queries

- Recommend configurations for the Network Management Systems (NMSs) of the Agency Network Operation Center (NOC) to monitor the IPv6 network and infrastructure
- Recommend configurations and/or upgrades for the Security Operation Center (SOC) for IPv6 security upgrades to monitor IPv4 and IPv6 threats
- Set up one or more applications that can run over IPv6
- Initially isolate the test sites from the production network and from each other

5.2.2 IPv6 Integration Testing in Test Lab

The FCC shall test the IPv6 integration of network infrastructure and applications in a lab environment:

- The FCC shall assess the networking equipment, recommend any needed upgrades, and work with the Agency to set up or configure per the IPv6 upgrade plan (IPv6 Deployment Strategy / Implementation Plan):
    1. Upgrade public/external-facing servers and services (e.g., Web, email, DNS, ISP services, etc.) to operate using native IPv6
    2. Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operate using native IPv6
    3. Support the Agency IPv6 Transition Manager in leading the transition activities, and liaison with the wider Federal IPv6 effort as necessary
- The FCC shall test IPv6 routing protocols for successful integration
- The FCC shall add minimum IPv6 support to critical networking services, including Domain Name Services (DNS) and Dynamic Host Configuration Protocol (DHCP) or auto-addressing as called for in the target architecture:
    1. The FCC shall develop and apply an IPv6 threats and countermeasures security policy that implements IPv6 security services (access control lists (ACLs), firewall, IDS, IPS, DMZ, and reporting) in accordance with the existing Agency security policies and rules.
    2. The FCC shall mitigate the following IPv6 threats, in accordance with the Agency security standards and regulations, such as DISA Security Technical Implementation Guides (STIGs), and if required through additional appropriate programming, security policies, and procedures:
        - Use of IPv6 to ex-filtrate data, facilitate malware, and enable botnet command and control infrastructures, undetected by IPv4-only sensors
        - Reconnaissance of device, network topology, and service discovery:
            - Reconnaissance is normally a precursor to an impending or future attack against the network, its devices, protocols and services, including network management, DNS and the security infrastructure
        - Layer Two Threats:
            - Spoofed Router Advertisements (RAs) can be used to renumber hosts on the segment or to launch a Man in the Middle (MITM) attacks and siphon off LAN traffic for capture
            - Forged Neighbor Advertisements (NA) and Neighbor Solicitations (NS) messages can be used to confuse Neighbor Discovery Protocol (NDP)
            - ICMPv6 Redirects, which are the same as IPv4 redirects
            - Forcing nodes to believe all addresses are on-link, i.e., denial of service (DOS) attack

    - Dynamic Host Configuration Protocol (DHCPv6) attacks involve providing false information during address negotiations with DHCPv6 servers
  - Layer Three Threats:
    - IPv6 Packet Header (base and extension) Manipulation and Fragmentation attacks evade security devices and attack network infrastructure, for example, IP header and packet modifications may include forging source addresses, incorrect sequences or a large number of nested extension headers, crafted packets with large chains of extension headers, separation of the payload into a second fragment and invalid extension headers. These can consume resources in a DOS attack.
  - Above Layer Four Threats:
    - Buffer overflows, cross-site scripting, SQL injection and email, spam, phishing and social engineering attacks
3. During IPv6 testing based on the Agency's IPv6 Transition Baseline, developed in the previous task, the FCC shall document successful configurations, interoperability issues and bugs found in a test log. The testing shall include:
   - IPv4-IPv6 dual-stack capabilities and all network and application services
   - Inserting failure conditions, such as router unavailability, DNS server misconfiguration, link outages, etc., to identify and document the behavior of networking and application elements
   - Exploring alternative workarounds to each simulated outage and observing the suitability of each resolution
   - Once the test scenarios have been completed, develop training material and labs, and cycle groups of IT staff through hands-on IPv6 training

5.2.3 Pilot Details & Success Criteria

The pilot will use two Dell OptiPlex 7070 workstations placed in the FCC Engineering lab on the 2nd floor of FCC HQ. The lab is connected to the building production network. The target services include address assignment and domain name lookup. IPv6 does not leverage Dynamic Host Configuration Protocol (DHCP) like IPv4; but, rather, incorporates a Stateless IP address autoconfiguration (SLAAC) that listens for Router Advertisement (RA) from the network and combines it with the local machines MAC address. The pilot will validate that IPv6 traffic can traverse the production NoMa network from Engineering Lab on the second floor, through the access switch, to the core switches to servers connected in wire closet on the 1st floor.

Each of the test factors will be addressed (below).

- VALIDATE THAT IPV6 IP ADDRESS ASSIGNMENTS ARE FUNCTIONING: The Dell OptiPlex workstations in the lab will receive Router Advertisement (RA) and correctly assemble their IPv6 address. The correct IPv6 address will be manually validated.
- VALIDATE THAT IPV6 TRAFFIC CAN TRAVERSE THE PRODUCTION NETWORK AT FCC HEADQUARTERS: The test workstations will perform a basic IPv6 "ping" to validate that they are getting IPv6 responses from devices located on the 1st floor.
- VALIDATE THE DELL OPTIPLEX WORKSTATIONS (FCC'S MAIN DESKTOP COMPUTER MODEL) ARE CAPABLE OF IPV6 WITH THE MICROSOFT 20H2 WINDOWS10 IMAGE: The previous two tests will validate that the OptiPlex workstations are capable of IPv6.

- VALIDATE THAT DOMAIN NAME SERVICE (DNS) SERVERS ARE ABLE TO USE IPV6: Manual DNS queries will be executed on the test machines to validate the in-building DNS server(s) are responding to queries correctly over IPv6.
- TEST EXISTING SECURITY STACK'S ABILITY TO DETECT, IDENTIFY, AND MANAGE IPV6 TRAFFIC: FCC's Cyber Team will review their security toolset to validate they can identify IPv6 traffic across the production network at NoMa.
- TEST LOADING A WEB PAGE OVER IPV6 FROM A TEST WEB SERVER INTERNAL AT FCC HQ: Using a browser, the workstations will load and render a static web page from a test server in NoMa over IPv6.

The test above will satisfy all the test objectives identified. In order to complete the test above, four servers will need to be procured to house DNS and web servers at NoMa. These servers will be leveraged for both the IPv6 test and other local server vices required for the building.

5.3 Pilot Production Deployment on Selected LANs

The FCC shall conduct the main phases required to validate and move IPv6 to production as follows:

1 Conduct a pilot production deployment for one or more campus LAN segments or for the WAN, as appropriate for the Agency's business mission
2 Expand the geographic reach of IPv6 by deploying it more broadly in the LAN/WAN environment and using it for Internet connectivity

At the conclusion of this phase, the FCC will be able to demonstrate IPv6 compliance in terms of the OMB mandate (i.e., the FCC can perform at least the following functions without compromising its IPv4 capability or network security):

- Transmit IPv6 traffic from the Internet and external peers through the network backbone (core) to the LAN
- Transmit IPv6 traffic from the LAN through the network backbone (core) to the Internet and external peers
- Transmit IPv6 traffic from the LAN through the network backbone (core) to another LAN (or another node on the same LAN)

5.3.1 Selected LANs and WANs

The FCC shall conduct a pilot production deployment for one or more LAN segments and for the WAN, as appropriate for the Agency's business mission, as follows:

- Since the Pilot involves the FCC's production network, this activity shall be done during non-business hours (e.g., during evenings and weekends) so that normal operations are not affected. In case of an adverse effect, it shall be possible to roll back to the previous condition so that normal operations are not affected.
- Set up routers and switches to process IPv6 traffic. Configure the LAN to transport the Agency's IPv6 prefixes to production host computers, printers, and other devices, including IPv6 routing protocols.
- Ensure that the security architecture is configured to handle both IPv4 and IPv6. Set up the DNS and DHCP servers to handle IPv6 queries.

- Ensure that the associated Network Management Systems (NMSs) are configured to monitor the IPv6 network and infrastructure.

1. Ensure that Agency WAN is dual stack:
   - If the Networx contract is used for the Agency WAN, Networx is already in compliance with the OMB IPv6 directive by providing an IPv6-capable core with dual-stack Provider Edge (PE) routers and protocol-independent tunnels (e.g., MPLS) between the POPs.
2. Set up one or more applications to run over IPv6 using the following sequence:
   - Assess host and server operating systems and applications
   - Select operating systems and applications that need to be upgraded or configured to operate over IPv6
   - Configure naming services to make selected applications available over IPv6
   - Begin operating and monitoring the applications over IPv6
   - Secure IPv6 on hosts
   - Test new applications and services, such as peer-to-peer communications and auto-discovery, that can enhance Government applications and services by supporting mobility, security, quality of service (QoS), and multicast

5.3.2 Selected LANs, WANs, and the Internet

The FCC shall deploy IPv6 more broadly in the LAN/WAN environment, and use it for Internet connectivity as follows:

- Since it involves the FCC's production network, this activity shall be done during non-business hours (e.g., during evenings and weekends) so that normal operations are not affected; in case of an adverse effect, it shall be possible to roll back to the previous condition so that normal operations are not affected
- When the production LAN pilot deployment is complete, connect the sites across the WAN, applying lessons learned from the pilot deployment; after testing the IPv6-capable applications, make them available throughout the FCC
- Connect to the Internet:

1. At this phase of the IPv6 integration, ensure that the FCC is now using dual stack routers for Internet connectivity. Configure the existing network infrastructure (intranet, DMZ, extranet, and Internet) to block or allow IPv6 traffic as appropriate. If the FCC is already using IPv6 tunnels, limit this capability to a few well-known routers.
2. Test for security with external IPv6 sites for the following scenarios:
   - IPv6 client behind the firewall connecting to an IPv6 resource on the DMZ
   - External IPv6 client connecting to an IPv6 resource on the DMZ
   - IPv6 client behind the firewall connecting to an IPv6 resource on the Internet
   - External IPv6 client connecting to an IPv6 resource behind the firewall
3. Begin operating and monitoring applications that use IPv6 when accessing IPv6 sites, such as Internet Explorer and Mozilla Firefox.
4. Monitor IPv6 traffic on an ongoing basis for problems.

5.3.3 IPv6 Deployment to Production

After a successful broad deployment involving multiple LANs, WAN and the Internet, and after demonstrating compliance with the OMB IPv6 mandate, the FCC shall transition the remaining network infrastructure to IPv6, including hardware, software, IPv6 address assignments, IPv6 services (DNS, DHCPv6) and IPv6 security; after the infrastructure changes are complete, FCC IT must perform a final checkout to ensure that the production network is ready for full IPv6 deployment. In addition, the FCC shall deploy per the timelines per OMB M-21-07. The FCC shall perform IPv6 changes/upgrades to the rest of the infrastructure to complete the IPv6 production deployment as follows:

- Since it involves the Agency's production network, this activity shall be done during non-business hours (e.g., during evenings and weekends) so that normal operations are not affected. In case of an adverse effect, it shall be possible to roll back to the previous condition so that normal operations are not affected.
- The FCC shall validate all system configurations and test the network before the configurations are loaded onto Agency production networks. If the network has different levels of security or sensitive information, then different network management and provisioning systems may be employed to control different domains. Some Internet-facing servers and systems may need isolated network management and provisioning to maintain security domains.
- The FCC shall finalize IPv6 upgrades to the Agency NOC and SOC and shall ensure that the Agency NOC and SOC are totally integrated for IPv6 deployment in the Agency's production network.
- The FCC shall finalize upgrades to all hardware and software, including IPv6 address assignments, IPv6 services (DNS, DHCPv6), and IPv6 security.
- The FCC shall finalize the upgrades to host and server operating systems.
- The FCC shall ensure that both internally developed and commercial management applications are fully operational over IPv6.
- The FCC shall ensure that the Data Center is fully operational for IPv6, including load balancing, Web server and WAN optimization solutions.
- The FCC shall upgrade specific solutions to IPv6, such as IP telephony.
- The FCC shall enable required IPv6 services such as DNS and DHCPv6.
- The FCC shall enable IPv6 routing within the enterprise.
- The FCC shall establish external IPv6 connectivity (Internet, Internet2, DREN, and to other agencies).
- After the final checkouts, the FCC shall complete the deployment of IPv6 throughout the infrastructure.

6. Implementation Strategy

6.1 Defined Targets

The OMB M-21-07 memo outlines 20%, 50%, and 80% targets for devices configured for IPv6 by FY23, FY24, and FY25, respectively. Specific language from the memo indicates "AT LEAST [XX]% OF IP-ENABLED ASSETS ON FEDERAL NETWORKS ARE OPERATING IN IPV6-ONLY ENVIRONMENTS BY THE END OF FY 202[X]". FCC

interprets “IP-enabled asset” to mean a device or instance connected to an FCC managed network that is IP-enabled. This would include:

- Infrastructure equipment (including routers, switches, firewalls)
- Host computers (including Thin clients, desktops, tablets, mobile devices)
- Servers (including physical servers, virtual servers)
- Environmental control devices (including UPS, CRAC units)
- Cloud instances and Services (including SaaS, PaaS, and IaaS instances, and services such as AWS, Azure, ServiceNow)
- Security devices (including Security cameras, electronic door locks, turnstiles)
- OT devices (including sensors, appliances)

This would not include devices or instances not leveraging IP and not managed by FCC, such as:

- Telephony provider networks
- Bluetooth devices
- Sensors and devices using non-IP based protocols

The expectation is that the device in question must operate in IPv6-only mode in order to meet the language in the OMB memo. This represents a challenge for infrastructure and security devices as they need to support IPv4 until all host devices are transitioned.

6.1.1 FY21 - PILOT

In order to achieve the pilot, the following requisites must be completed:

- IPv6 addressing plan developed and approved
- IPv6 network configuration implemented at NoMa (at minimum, partially)
- Servers for local NoMa services be procured, implemented, and configured for DNS and web services using IPv6
- Three existing OptiPlex workstations be installed in the engineering lab with updated Windows10 20H2 based image and configured for IPv6
- Firefox or Chrome browsers be installed on the OptiPlex workstations

6.1.2 FY23 - 20% TARGET

To meet the OMB 20% target by end of FY2023, the recommendation is to focus on end-user computing devices and the IGEL thin clients. These devices are new, and hardware and IGEL software support IPv6. Although the Windows desktops in Azure (Cloud VDI) will not be IPv6-enabled, the thin client access from NoMa will be set up for IPv6-only. There are about 1,300 Dell Wyse Thin Clients at NoMa so this will go a long way to satisfy the 20% IPv6 requirement and, if prioritized, could be completed in FY22 - one year ahead of the OMB requirement. To achieve the 20% target with the Wyse device the following must be completed:

- Pilot completed successfully
- IPv6 is enabled and working on the NoMa networks

- Local DNS installed at NoMa and functioning with IPv6 dual stack
- WAN configured and tested for IPv6
- This is required for communications to AWS (IGEL console) and Azure (Cloud VDI)
- Security devices
- A subset of the security components must be IPv6 enabled
- IGEL software IPv6 compliance verified, validated, and implemented
- Dell Wyse 7070 IPv6 compliance verified, validated, and implemented
- AWS configured for IPv6 for IGEL console (dual stack)
- Azure configured for IPv6 for Cloud VDI (dual stack)
- Project prioritized, funded, and staffed.

Another target for the FY2023 20% IPv6 compliance requirement is the Cisco 8851 phones deployed at NoMa and GB (phones connecting to Cisco UCM Cloud). The phones are new and support IPv6 and the UCM Cloud Service can be configured for dual stack. To add the phones to the 20% requirement and to succeed in the 2023 target, the following is required (in addition to the steps above):

- WAN Phone VRFs configured for IPv6 dual stack
- Telephony infrastructure at FCC configured for dual stack
- Cisco UCM service configured for dual stack

There are approximately 1,500 phones installed at NoMa that, with the IGEL devices, represents >20% of all IP-enabled devices in the infrastructure. The configuration to move to IPv6 for the 8851 phones and dual stack for Cisco UCM Cloud is achievable in FY22 if the project is prioritized, funded, and staffed properly.

6.1.3 FY24 - 50% TARGET

To meet the 50% compliance requirement by the end of FY2024, the recommendation is to transition the FCC desktop computing services (currently Windows10) desktops, both VDI and physical, before the end of FY2024.

The FCC has greater than 2,100 active desktops; IGEL devices, Cisco Phones, and Windows desktops represent greater than 50% of all IP-enabled devices in the enterprise. A complete device inventory is required to ensure compliance with OMB mandate. To support the significant inventory of legacy services, an IPv6/IPv4 gateway or other translation service must be implemented in order to configure the desktops in IPv6-only mode. It is also highly likely that in FY2024 FCC will still have legacy desktop applications that are not IPv6 compliant; although, this will not likely represent a majority of users. Resolutions steps are (in rank order):

- Leverage host based IPv6/IPv4 translation services
- Replace non-compliant software with alternative solutions
- Keep an approved subset of desktops in dual-stack mode

To support the gradual transition of desktop and desktop applications to IPv6, it is recommended to:

- Enable dual stack (target FY2022/2023)
- Enable IPv6-only for Cloud VDI (target FY2023/2024)

- Enable IPv6-only for full desktops (target FY2024)

To achieve the 50% target by the end of FY2024 the following is required:

- 20% target met
- Device inventory completed and validated
- All network services and infrastructure are enabled for IPv6
- All Core services (DNS, Active Directory, Authentication) are enabled for IPv6
- All security infrastructure supporting IPv6
- All monitoring services supporting IPv6
- IPv6/IPv4 translation gateway or other translation services enabled
- Desktop software inventory completed and IPv6 compliance validated
- Host based IPv6/IPv4 translation implemented
- Software distribution solutions supporting IPv6

6.1.4 FY25 - 80% TARGET

In order to meet the 80% target, set by OMB by end of FY2025, the recommendation is to focus on business application components and Cloud service providers such as AWS and Azure. A complete Cloud service provider list should be maintained, and IPv6 compliance plans tracked. Both Azure and AWS already support IPv6 and the implementation is maturing and expanding to all offered services.

A complete business and support system inventory with technologies needs to be developed, tracked, and validated for IPv6 compliance and a transition plan needs to be created. This will also be incorporated with the Cloud Modernization Plan and, as systems are migrated, they will be made IPv6 accessible. To achieve the 80% target with the business applications in AWS and Azure Cloud services, the following must be completed:

- 50% compliance met
- Complete inventory of systems and technologies developed and validated for IPv6 compliance
- Transition plan developed regarding technology and device basis

7. Implementation Support

7.1 Infrastructure & Data Support

7.1.1 Hardware

Instructions: Provide a list of hardware thought to be necessary for implementation to occur.

Hardware inventory lists with relevant IPv6-readiness statuses shall be provided by the following IPT Members:

- Tailored Platforms & Data
- Cloud Integration and Catalog
- Enterprise Operations & Services

- Information Security & Resiliency

Each of the above IPT members shall analyze the software/data needs to be upgraded, replaced, or enabled for IPv6, and classified along one of the following categories:

- Currently running IPv6
- IPv6-compliant but device needs to be configured for IPv6
- Requires software upgrade for IPv6 compliance
- Requires hardware upgrade to support software upgrade
- Legacy platform: cannot be upgraded to support IPv6 and must be replaced
- Will not be upgraded due to planned discontinuation

7.1.2 Software

Instructions: Identify any software that will be used to facilitate the implementation process, such as software specifically designed for automating the installation process.

Relevant FCC FTEs, and contractors shall analyze the software/data needs to be upgraded, replaced, or enabled for IPv6, and classified along one of the following categories:

1. Currently running IPv6
2. IPv6-compliant but device needs to be configured for IPv6
3. Requires software upgrade for IPv6 compliance
4. Requires hardware upgrade to support software upgrade
5. Legacy platform: cannot be upgraded to support IPv6 and must be replaced
6. Will not be upgraded due to planned discontinuation

7.1.3 Data

Instructions: Describe specific data preparation requirements and data that must be available for the system or situation implementation. An example would be the assignment of individual IDs associated with data preparation.

Relevant FCC FTEs, and contractors shall analyze the software/data needs to be upgraded, replaced, or enabled for IPv6, and classified along one of the following categories:

- Currently running IPv6
- IPv6-compliant but device needs to be configured for IPv6
- Requires software upgrade for IPv6 compliance
- Requires hardware upgrade to support software upgrade
- Legacy platform: cannot be upgraded to support IPv6 and must be replaced
- Will not be upgraded due to planned discontinuation

7.1.4 Facilities

The IPv6 Implementation Program affects the FCC Enterprise, which includes HQ2 and Gettysburg facilities. FCC IT will conduct implementation via HQ2.

The IPv6 Workstation Test Lab is located on the second floor of HQ2.

7.2 Performance Monitoring

Instructions: Describe the performance monitoring tools and techniques that will be utilized during implementation and explain how they will be used to measure success versus failure.

Projects that fall under the FCC IT Project Management Office (PMO) are subject to reviews by the PMO and Enterprise Planning & Performance (EPP) groups.

7.3 Configuration Management

Instructions: Describe the configuration management protocol that will be followed and the procedures that will be used for configuration control, change control, and configuration status account reporting.

New acquisitions and newly activated features to existing assets may be subject to the FCC's Solutions Development Framework (SDF) lifecycle processes. The Senior Project Manager will consult with the Business Lead and Project Team to confirm respective gates and documentation. From there, the Senior Project Manager will direct lifecycle actions on behalf of the Project Team.

8. Security and Privacy

New acquisitions and newly activated features to existing assets will be subject to the FCC's Solutions Development Lifecycle (SDLC) processes to confirm for security and privacy ramifications.

9. Reference Documents

Table 6. Reference Documents

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
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 IPv6 Compliance Policy	https://www.fcc.gov/sites/default/files/fcc-it-ipv6-compliance-policy.pdf
FCC IT Procurement Check List	https://www.fcc.gov/sites/default/files/fcc-it-ipv6-procurement-checklist.pdf
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 (1Pv6), November 2020 https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

Appendices

Instructions: Add or link any supporting documentation for this project as needed.

Appendices pending.