HexaBuild

White Paper - IPv6 Strategy for State Governments and U.S. Federal Agencies

Prepared For: HexaBuild Customers and Partners

Prepared By: Tom Coffeen, Scott Hogg, Ed Horley, Tim Martin, and Steve Rogers

Date: February 22, 2021

Filename: HexaBuild White Paper - State and Federal IPv6

HexaBuild, Inc.

Table of Contents

1. White Paper Summary

This paper will cover the topic of adopting Internet Protocol version 6 (IPv6) in U.S. Federal agencies and State governments. It will discuss the impacts of compliance as well as some of the use cases and examples to successfully adopt IPv6. The goal is to raise awareness of the Federal mandate and relate it to some of the challenges that a Statewide network may encounter when connecting to U.S. Federal agencies in the future.

HexaBuild is uniquely positioned to help governments learn, design, and deploy IPv6 with a focus on Cloud, IoT and Security. With over 80 years of combined IPv6 experience our team has designed, deployed, operated, and worked on IPv6 since the early adoption of the protocol. This includes participation in the US Federal IPv6 Task Force and the NIST standard for IPv6 Security (800-119). As we enter 2021, many organizations are starting to realize they lack the skills and expertise to adopt IPv6 correctly the first time. HexaBuild is here to help your team get IPv6 up and working in your environment. You can download the HexaBuild IPv6 Adoption report at https://www.hexabuild.io/downloads.html for more information about the current shift to IPv6 happening on the Internet.

2. U.S. Federal Government IPv6 Mandate

Overview

On Nov 19, 2020 the U.S. Federal Government via the Office of Management and Budget (OMB) has released a memorandum focused on the deployment of the Internet Protocol version six (IPv6).

The Office of Management and Budget (OMB) Memo M-21-07

The memo can be found at:
https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf

Important sections to highlight from this memo include the following:

1. Issue and make publicly available an agency-wide IPv6 policy by June 2021; require all new networked systems be IPv6-enabled by the end of FY2023 and have a strategic plan for removing IPv4
2. Complete and report on at least one IPv6-only pilot project by the end of FY2021

3. Develop an IPv6 implementation plan to fully enable native IPv6 operation by the end of FY 2021
4. Develop an IPv6 implementation plan by the end of FY 2021, and update the Information Resources Management (IRM) Strategic 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 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;*

* Italics added for emphasis.

3. U.S. Federal Government

This memo is directed at all branches of the U.S. federal government and impacts how the U.S. government will adopt IPv6. The memo requirements pose several challenges for federal agencies. Specifically:

1. The need to build and operate an IPv6-only lab for testing and validation
2. Submission of a plan to adopt and deploy IPv6
3. The ability to support and operate a portion of their network IPv6-only
4. The ability to measure and report on their progress
5. Training and educating their technical staff
6. Design and architecture of IPv6

The key point of this Federal memo is that the U.S. Government is now developing plans to disable use of the legacy IPv4 protocol. The requirements for IPv6-only lab testing and making production environments IPv6-only will end up making IPv6 the dominant and preferred protocol for communication within, between, and external to Federal departments and agencies.

These requirements differ from what states will need to address regarding IPv6.

4. State Government

While the memo does not directly instruct any state about IPv6 adoption (nor could it without congressional approval) it will indirectly impact all states due to the nature of the adoption requirements for the federal agencies. All states will need a specific strategy and roadmap for IPv6 adoption as a result of these Federal mandates but will have more flexibility and discretion about how to do the adoption. We have identified the following challenges for states:

1. IPv6 adoption to meet the growing demands of state and local agencies
2. Addressing security concerns and vulnerabilities while adopting IPv6
3. Compliance and interface requirements to the U.S. Federal Government
4. Funding and resource allocation
5. Training and educating technical staff
6. Design and architecture of IPv6

This list is not inclusive of all the challenges but gives a good example of the common ones that state and local government will face. The goals for states will be the continued ability to transact network traffic with the U.S. government as they adopt IPv6. This will require states adopt IPv6 and appropriate transition technologies to ensure access to funds, services and communication with the U.S. federal government.

Role of the State CIO (with an Eye on Security)

IT modernization has many facets including cloud migration, IoT, cybersecurity and the enablement of the modern Internet Protocol (IPv6). All modern operating systems ship with IPv6 enabled and preferred by default. Within the standards bodies focused on IoT, IPv6 is the preferred network stack (i.e., 6LoWPAN, Thread). The modernization plan of any network should include:

- A plan for IPv6 adoption
- Preparation to support both legacy and modern devices
- Staff training to operate IPv6 effectively

State agencies must properly identify their incoming and outgoing web traffic, anticipate threats, and defend the network to prevent future breaches.
This threat surface continues to expand with modernization. From a security perspective, it is best to enable and lock down all protocols including IPv6.

To do this best, a deep understanding of IPv6 must be learned by the staff supporting these networks. Operational knowledge and best practices are also critical to allow for efficient uptime and availability of the network. IPv6 skills for host operating systems, networks, applications, help desk and other roles will become critical and the adoption requirements expand. Proper planning on the phased adoption of IPv6-only or Dual-Stack will be critical along with policies and procedures to ensure hardware, software and cloud solutions that are purchased by the state and Local governments have IPv6 support.

5. Functional Examples of State and Federal Agency Interactions

The following examples highlight efforts that State and Federal Agency have taken related to the topics of STEM, Economic, and Law Enforcement related to IPv6.

Science, Technology, Engineering, Mathematics - STEM

State and local agencies should utilize STEM funding initiatives to help supplement their IPv6 project budgets. These can be tied to National Science Foundation (NSF) grants and other agencies who already (NSF), or soon will, require IPv6 to connect and exchange information.

“In an ever-changing, increasingly complex world, it's more important than ever that our nation's youth are prepared to bring knowledge and skills to solve problems, make sense of information, and know how to gather and evaluate evidence to make decisions. These are the kinds of skills that students develop in science, technology, engineering, and math, including computer science.” - US Department of Education.

National Science Foundation (NSF)
The Campus Cyberinfrastructure (CC*) program invests in coordinated campus-level networking and cyberinfrastructure improvements, innovation, integration, and engineering for science applications and distributed research projects. Learning and workforce development (LWD) in cyberinfrastructure is explicitly addressed in the program. Science-driven requirements are the primary motivation for any proposed activity.

“Preference will be given to proposals describing an operational role for IPv6, for example, describing native IPv6 support for one or more specific science applications.” - from NSF 16-567

The migration towards IPv6 helps fulfill this mission and helps maintain America’s leadership in Internet technologies.

Economic Stewardship and the US Dept. of Treasury

The U.S. Department of the Treasury manages the nation’s finances by collecting money due to the United States, making its payments, managing its borrowing, investing when appropriate, performing central accounting functions, and printing money. The department also provides State Governments with economic aid in varying forms. The department is fully enabled with IPv6 addressing and technology. Many of the “touch points” from State Governments will benefit from aligning to the modern Internet Protocol, with increased performance, enhanced security, and greater scalability.

Law Enforcement and the National Database

The National Crime Information Center (NCIC) has been called the “lifeline of law enforcement”. State and local justice agencies enter records into NCIC that are accessible to virtually all law enforcement agencies nationwide. A law enforcement officer can search for warrants, stolen property, identify terrorists, locate missing persons and allow for them to perform their duties more safely. Since this system is accessed in real time, performance and a quick reply is essential to officer safety. The NCIC and its components are IPv6-enabled, providing the most secure, most reliable and fastest response over the modern Internet Protocol.

6.Skills, Education and Training

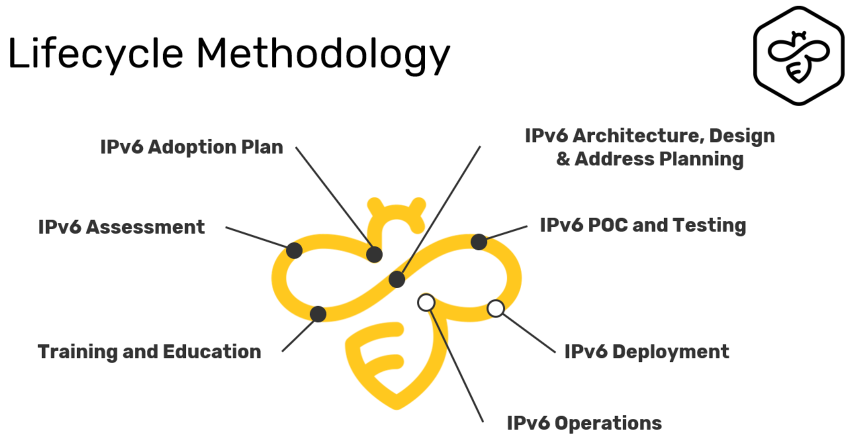
Most agencies have not invested significant time or money into training their existing IT staff on IPv6. These skills are critical in order to be able to implement, operate, and support IPv6-only or dual-stack networks.

What to do

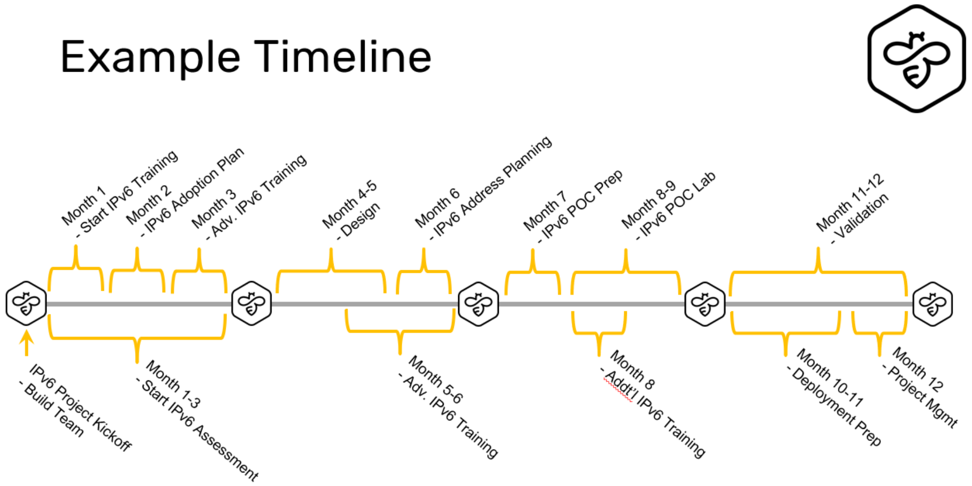
The challenges that arise from the OMB memo can be addressed by doing the following activities and tasks based on the HexaBuild Lifecycle Methodology:

1. Build an IPv6 adoption plan and assemble your team
2. Complete an IPv6 capabilities assessment
3. Engage with IPv6 experts for training and education on IPv6
4. Architecture, design and address planning
5. Build an IPv6-only Proof of Concept (PoC) lab (physical or virtual)

These steps are shown the following diagram:



To accomplish these steps, a project plan needs to be utilized to have a successful deployment and adoption of IPv6. The following is an example timeline to show what steps our previous IPv6 projects completed and when.


Example Timeline
Month 1 - Start IPv6 Training
Month 2 - IPv6 Adoption Plan
Month 3 - Adv. IPv6 Training
Month 4-5 - Design
Month 6 - IPv6 Address Planning
Month 7 - IPv6 POC Prep
Month 8-9 - IPv6 POC Lab
Month 11-12 - Validation
IPv6 Project Kickoff - Build Team
Month 1-3 - Start IPv6 Assessment
Month 5-6 - Adv. IPv6 Training
Month 8 - Addt'l IPv6 Training
Month 10-11 - Deployment Prep
Month 12 - Project Mgmt

Engaging HexaBuild for the Solution

If your agency is planning on pursuing an IPv6-only PoC lab, it is critical to perform the planning step now. It is easier and less costly to perform this planning now rather than wait until you need to turn up IPv6-only services. Failure to prepare for this ahead of time could potentially delay compliance with the OMB memo mandates. Your organization needs to be proactive if you want to be able to comply in the next 12 months. HexaBuild is here to help and ready to engage with you to streamline your IPv6-only strategy.

HexaBuild, Inc.

11201 N Tatum Blvd., Suite 300
PMB 51634
Phoenix, AZ 85028-6039

+1 (415) 275-1066

https://hexabuild.io

Document date: 2021-2-22-A
Document version: 1.0