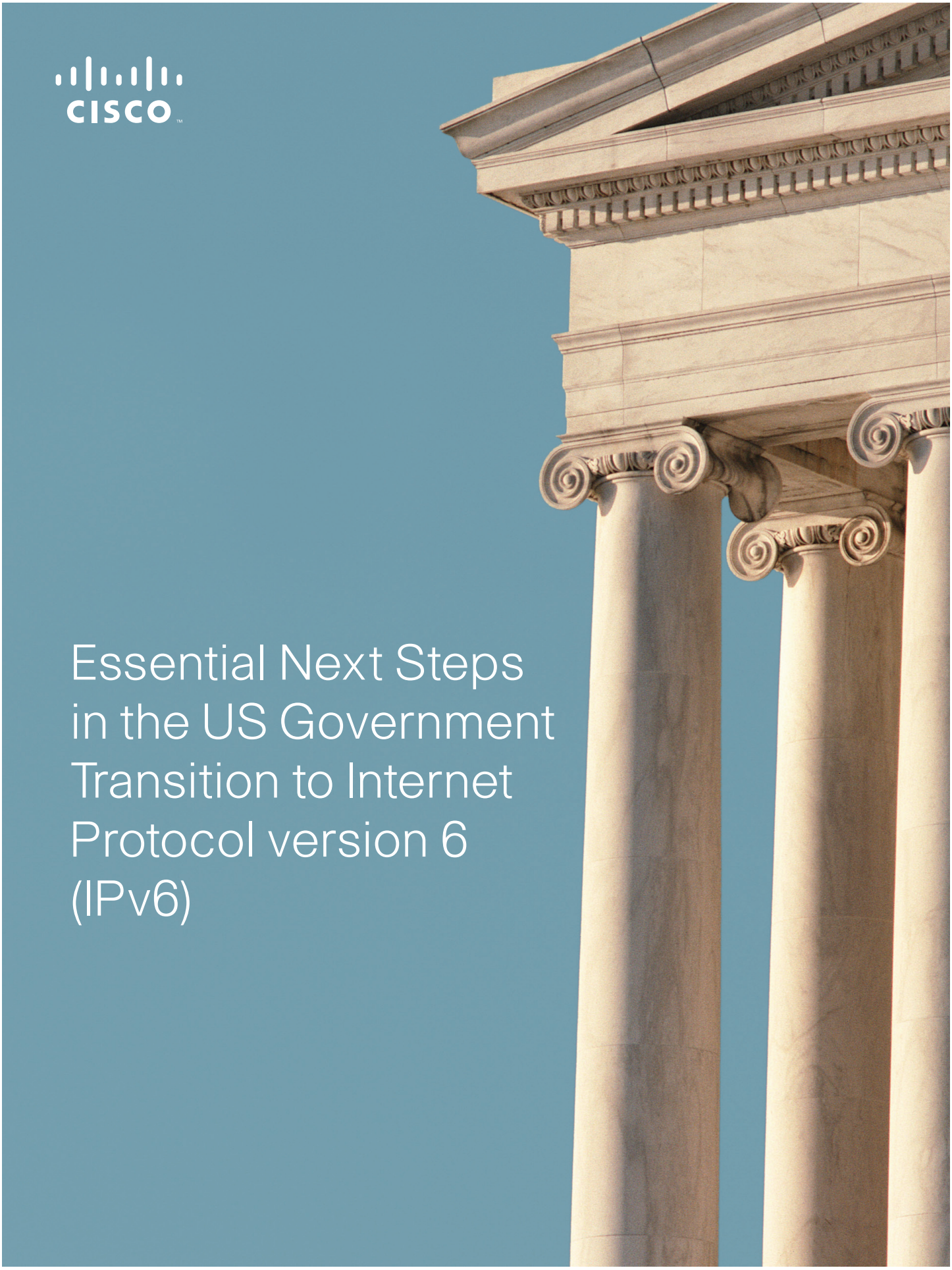


Essential Next Steps in the US Government Transition to Internet Protocol version 6 (IPv6)

An Executive Summary for Agency Chief Information Officers (CIO) of the Latest Federal Policies and Guidance for Continuing the Enterprise Transition to IPv6

September 2009

The United States Government (USG) has committed to and made significant progress in the transition to the next-generation Internet standard IPv6. Recently, a series of new policies and guidance have been released from several sources on the next steps agencies need to take in their continuing transition to IPv6. This guide provides federal CIOs and IT staff with a summary of the requirements and next steps you should be considering as you migrate your agency's enterprise Infrastructure to IPv6. This document provides the executive reader with a:

- High-level summary of federal requirements and guidance for transitioning to IPv6
- Clear set of next steps that you should consider for your agency's IPv6 transition
- Set of checklists to help prioritize next steps in your agency's IPv6 transition
- Timeline to understand the federal IPv6 roadmap

Understanding the Federal IPv6 Framework

The Internet and its related technologies have had a profound impact on business, government, and the social fabric of the United States and the world. Much of our economy, government, and entertainment are now directly or indirectly serviced using the Internet. No other technology has allowed for the level of collaboration and innovation that has occurred over the past two decades, and its potential has been only partially realized. The current Internet Protocol (IPv4) was never intended to provide the level of scalability and capability that has been achieved today, much less meet the exponentially increasing demands of tomorrow. Thus, IPv6 was created to succeed IPv4 and provide for a foundational shift in the IP architecture that will allow for continued innovation and change to meet the ingenuity of future generations.

The USG began the formal process of adopting IPv6 in 2003 and has met the initial milestones laid out by OMB and other USG leaders, with successful agency testing culminating in June 2008. With new guidance and policy being released by OMB, NIST, and the CIO Council, agencies must now begin moving from IPv6 trials into IPv6 operations. At the same time, the new administration has begun to establish aggressive goals that rely upon technology innovation to improve agency performance. This provides the perfect opportunity for you to prepare your network for the next-generation applications that will leverage the benefits of IPv6 while meeting the demands of excellence placed upon you by the new administration.

As shown in Figure 1, many new policy and guidance documents have been released over the past 12 months that provide significant direction to federal CIOs. This will impact your future agency enterprise network architecture and the overall method by which government procures IT hardware and software. It is not enough to have a small team focus on IPv6; it must now be integrated into the way your agency does business to continue to be successful.

This document provides a high-level overview of the next steps you should take in developing your agency's IPv6 transition and overall roadmap, and takes into account the policy and guidance from the most recent federal authoritative sources, as summarized in Table 1 and Table 2.

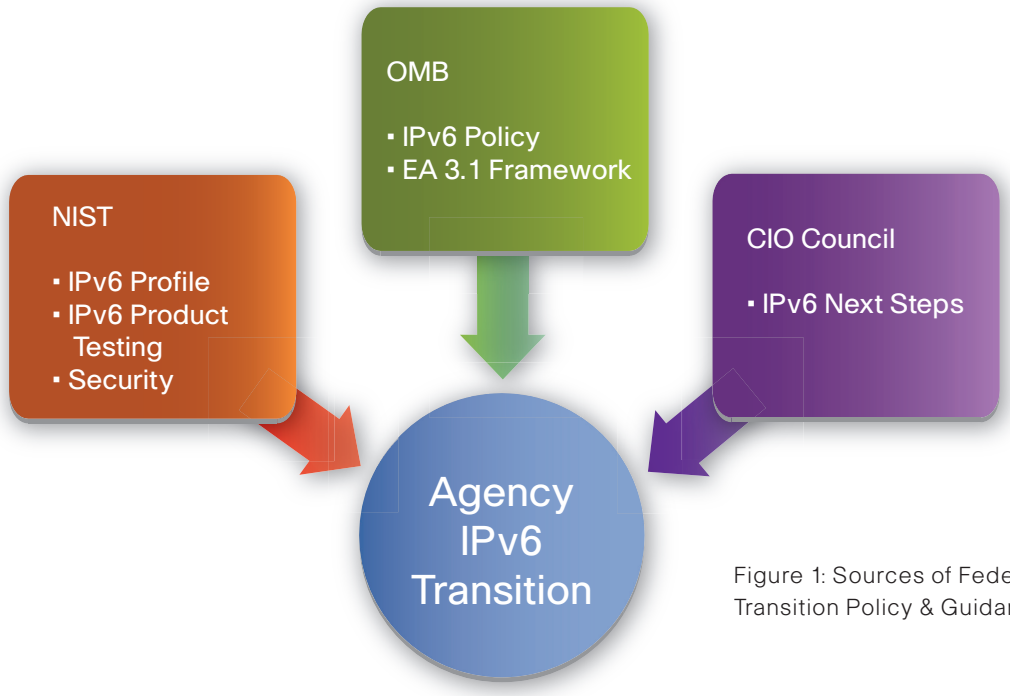


Figure 1: Sources of Federal IPv6 Transition Policy & Guidance

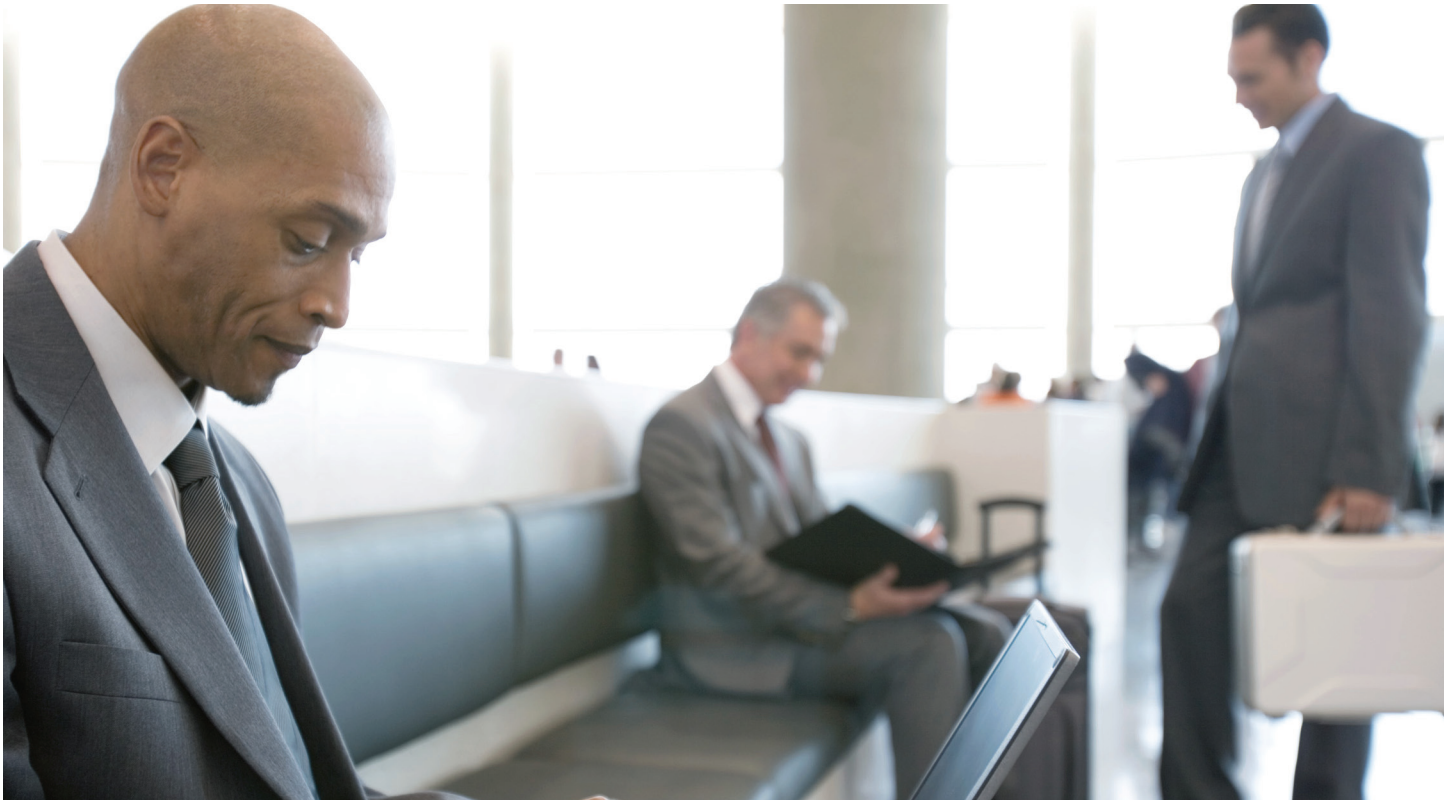
IPv6 creates a Service Oriented Infrastructure (SOI) that provides greater flexibility and agility to support innovative technologies such as Cloud Computing, virtualization, Green IT, and Service Oriented Architecture (SOA).

Table 1: US Government IPv6 Policy and Guidance Quick Reference Guide & Checklist

Title	Significance	Checklist
NIST: Special Publication (SP) 500-273: IPv6 Test Methods: General Description and Validation – Version 1.0, August 2009	Establishment of a federally approved IPv6 test program in conjunction with NIST SP 500-267 to support the acquisition of IPv6 hardware and software	· Inform Vendors of Plans to Support NIST IPv6 Product/Testing Programs · Identify Certified IPv6 Test Lab Approach · Update Acquisition Policy to Include IPv6 Profile and Test Requirements · Required Vendors Self Declaration of Conformance for IPv6 Acquisitions · Train Technical and Acquisition Staff on IPv6 Test Process and Requirements
OMB: Improving Agency Performance Using Information and Information Technology (Enterprise Architecture Assessment Framework v3.1), June 2009	Identifies agency enterprise architecture reporting requirements with a significant emphasis on IPv6	· Level 1: IPv6 Cost/Risk Impact Analysis & 2nd IP Device Inventory · Level 2: Evidence of Meeting IPv6 Transition Milestones · Level 3: IT Infrastructure Segment Architecture with IPv6 Included · Level 4: Exhibit 300 for IPv6 Enabled Network Services · Level 5: Exhibit 300 for IPv6 Enabled Mission Service/Application
CIO Council: Planning Guide/Roadmap Toward IPv6 Adoption within the US Government Version 1.0, May 2009	Latest guidance to Agencies from the CIO Council and OMB to support the transition to IPv6	· Agency Business Rationale for IPv6 · Identify IPv6 End User Applications · Quarterly IPv6 EA Assessment Reporting · Agency IPv6 Transition Milestones · IPv6 Integration with Federal Initiatives
NIST: Special Publication (SP) 500-267: A Profile for IPv6 in the U.S. Government – Version 1.0, July 2008	Technical profile to be used by the federal government to support the acquisition of IPv6 hardware and software	· Develop Agency Specific IPv6 Product Profiles · Compare Existing IPv6 Capable Products to IPv6 Product Profile · Train Technical and Acquisition Staff on IPv6 Profile Requirements · Work with NIST on Profile Effort

Table 2: Additional US Government IPv6 Policy and Guidance Documents

Title	Significance
DoD IPv6 Standard Profiles for IPv6 Capable Products Version 4.0, 2009	Technical profile to be used by the DoD to support the acquisition of IPv6 hardware and software
NTIA: Technical and Economic Assessment of Internet Protocol Version 6 (IPV6), January 2006	Assessment report by the Department of Commerce on the US Government transition to IPv6
OMB Memorandum: M-05-22Transition Planning for Internet Protocol Version 6 (IPv6), August 2005	Policy initiating the transition of civil agency networks to IPv6
DoD Memorandum: Internet Protocol Version 6 (IPv6) Policy Update, August 2005	Updated policy delineating specific milestone objectives for the DoD transition to IPv6
DoD Memorandum: Internet Protocol Version 6 (IPv6), June 2003	Policy initiating the transition of the DoD networks to IPv6



Use NISTs IPv6 product profile as a procurement guideline, but focus beyond just IPv6 compliance and determine how your solution will work together as an IPv6 system and address your agency's future requirements.

Federal IPv6 Transition Timeline

In order to maintain interoperability and promote innovation and collaboration, you must understand the high-level IPv6 transition schedule anticipated for the federal government and industry as a whole. The exhaustion of IPv4 addresses, coupled with the new features and benefits of IPv6, is driving not only the USG to adopt IPv6, but other governments and industry as well. Figure 2 displays the anticipated IPv6 phases and the timeliness of your agency's transition to IPv6.

The IPv6 acceptance cycle shows when IPv6 will be utilized across the USG and industry and when you should expect to focus on IPv6-only solutions. The IPv6 transition phases and timelines represent the current thought in the federal community on the steps and timeframes for the overall federal IPv6 transition. The figure provides a simplistic view that is focused on the initial enterprise infrastructure transition, and in reality the cycle will repeat for specific programs, development activities, and advanced IPv6 capabilities.

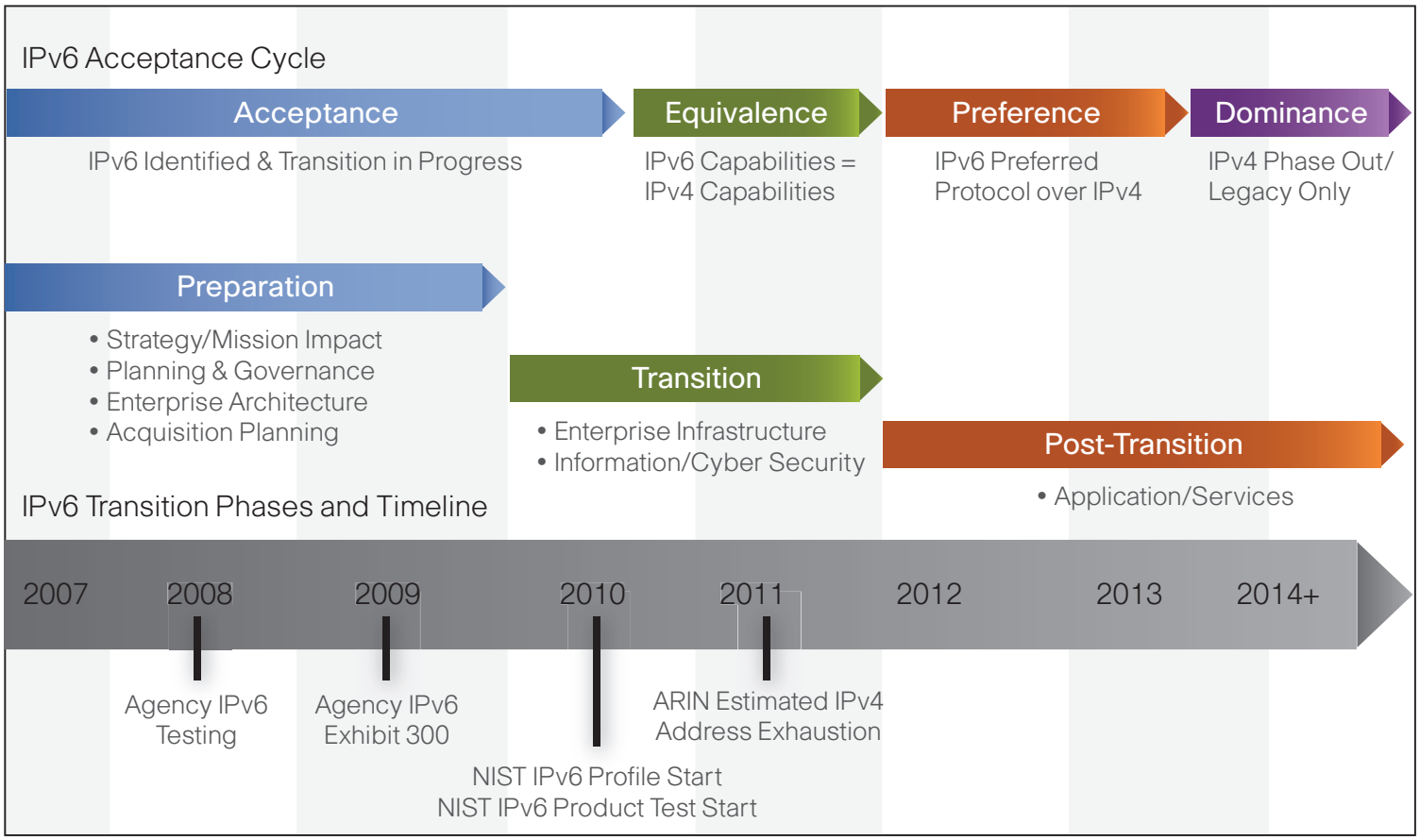


Figure 2: Federal IPv6 Transition Phases and Timelines

One of the most significant lessons learned from both government and industry is to develop an extended IPv6 transition approach that marries your technology refreshment cycle to save money and effort, and to reduce transition issues.

Agency IPv6 Next Steps and Roadmap

While there has been significant guidance developed within the federal community and in the public sector, transitioning to IPv6 is not a "one size fits all" methodology. Every agency has a unique mission and culture that must be reflected within its overall transition effort to be successful and achieve the best results. Agencies should leverage lessons learned and best practices from both the government and private sector.

This section presents a simplified plan of action taken from the federal IPv6 transition policy and guidance documents in Table 1. Figure 3 shows the cyclical process and steps of the federal IPv6 transition roadmap, and Table 3 provides a checklist of actions you should consider during each step. The challenge with IPv6 is that IP is such a pervasive technology and impacts the entire enterprise from routing and switching devices to applications, security, to end user devices. Eventually, any device or application that utilizes the network to communicate will be part of the agency's IPv6 transition plan. Thus, most of your initial IPv6 implementations will focus on providing basic IPv6 connectivity with advanced IPv6 capabilities being deployed over time as new applications and requirements are developed. While IPv6 is a next-generation technology, it has been standardized for over a decade and has been operationally demonstrated in government, academia, and commercial networks and enterprises.

You should integrate IPv6 transition and planning activities into your agency's major IT programs and initiatives. IPv6 will be the core transport protocol for all future communications and should be the basis for all new developments or enhancement. In addition, you should include IPv6 requirements and impacts on other federal initiatives such as:

- Trusted Internet Connection (TIC)
- Homeland Security Presidential Directive - 12 (HSPD-12)
- IT Infrastructure Line of Business (ITILoB)
- Federal Desktop Core Configuration (FDCC)
- Networx Migration
- Domain Name System Security (DNSSEC)
- Cloud Computing
- Transparency/Reporting
- Green IT/Health IT

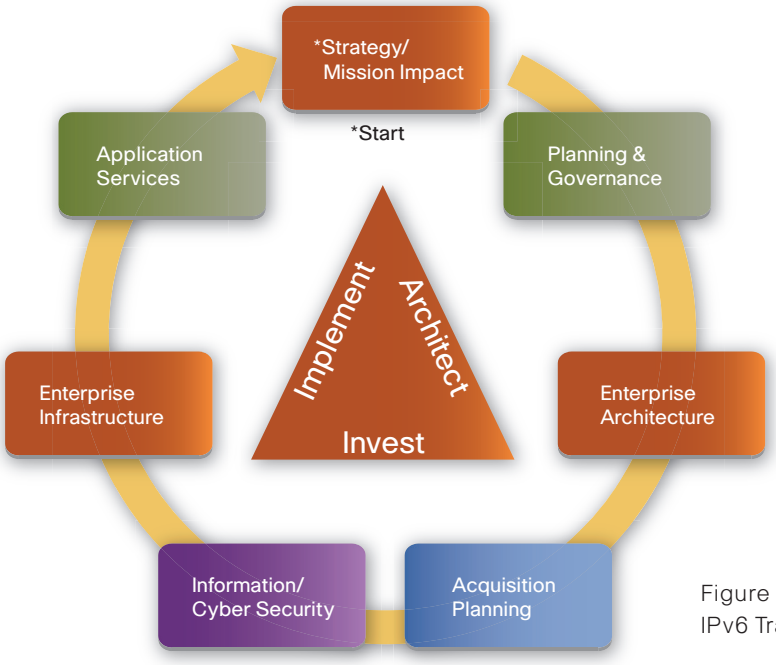


Figure 3: Summary of Federal IPv6 Transition Next Steps

OMB is utilizing the Federal Enterprise Architecture to monitor and manage the agency IPv6 transition progress. You should build IPv6 into the Capital Planning and Investment Control Process (CPIC) and Exhibit 300.

Table 3: Agency IPv6 Transition Steps Checklist

Title	Significance	Checklist
Strategy/ Mission Impact	· Map IPv6 Capabilities to Core Agency Mission & Goals · Identify Business Driven Need/Value for IPv6 within the Agency · Develop "to-be" IPv6 environment	· Assess "as-is" IPv4 & IPv6 environments identify the IPv6 gap · Develop the Agency IPv6 Business Case · Update Agency Strategic IT Plan to Include IPv6
Planning & Governance	· Updated IPv6 Transition Plan · IPv6 Transition Milestones · Updated/Second IP-Aware Device Inventory · IPv6 Cost & Risk Impact Analysis	· IPv6 Transition Policies · Agency-Wide IPv6 Transition Project Plan · Integration with Other Federal Initiatives (TIC, Networx Transition, FDCC, etc.) · IPv6/Technology Transition Office
Enterprise Architecture	· IT Infrastructure Segment Architecture with IPv6 Included · Enterprise Architecture Assessment Framework (EAAF) Quarterly Reporting · Evidence of IPv6 Transition Milestones Completion	· Integrate IPv6 with Capital Planning and Investment Control (CPIC) Process · Exhibit 300 for IPv6 Enabled Network Services · Exhibit 300 for IPv6 Enabled Mission Service/Application
Acquisition Planning	· Develop IPv6 Acquisition Strategy · Tie IPv6 Acquisition to Technology Refreshment Cycle · Become Aware of and Participate in NIST IPv6 Product Profile and Testing Programs · Consider IPv6 Contract Support Vehicle	· Inform Vendors of Plans to Support NIST IPv6 Product/ Testing Programs · Develop Agency-Specific IPv6 Product Profiles based on NIST SP 500-267 · Required Vendor IPv6 SDOC Based on NIST SP 500-273 for all IPv6 Acquisitions
Information/ Cyber Security	· Develop IPv6 Security Policies · Comprehensive IPv6 Security Plan · Include IPv6 in FISMA Reporting/Activities · Implement IPv6 C&A · IPv6 Security Awareness Program & Training	· IPv6 Enabled Firewalls/IDS/IPS · IPv6 Penetration Testing · Enable Host Based IPv6 Protection · Deny Rogue IPv6 Tunnels · Disable IPv6 by Default - Enable as Necessary
Enterprise Infrastructure	· Establish IPv6 Test Lab · IPv6 Addressing & Routing Plan · Acquire/Allocate/Manage IPv6 Address · Deploy Required IPv6 Transition Technologies · Enable IPv6 on External Facing Servers · Build IPv6 Operational Gap Analysis	· Implement IPv6 Simulation & Testing · Enable IPv6 Domain Name Service (DNS) · Implement DHCPv6 · Enable IPv6 Network Management · Provide IPv6 Desktop Access · Enable IPv6 on Internal & Gateway Routers
Applications/ Services	· Application Inventory · Legacy Operating System Assessment · Application Transition Milestones · Application Interoperability Planning · GOTS Application Transition Schedule	· COTS Application Transition Schedule · Application Developer Training · Application Laboratory · Application Testing · Application Transition Guidance

Your security policies, products, and plans should include IPv6 today to prevent breaches that can occur from unknown or unauthorized use of IPv6 within the enterprise.

Summary

Many agency CIOs find that their priorities are much higher than their resources or funding can handle and are quick to put off tasks that are not mission critical for future consideration. Delaying internal IPv6 coexistence and deployment practices can create a devastating effect on the agency by dramatically increasing the cost and potential operational impacts in enabling IPv6. From an acquisition perspective, at a minimum you should require that all new IT purchases and development meet the NIST IPv6 product profile requirements, even if there are no plans to immediately deploy IPv6.

Many organizations such as Google, Defense Research and Engineering Network (DREN), Internet2, and Nippon Telephone & Telegraph (NTT) have IPv6 enabled in their networks and use it operationally on a daily basis. They have reported that implementing basic IPv6 services was not difficult or expensive. It would be beneficial for you to create an IPv6 operational baseline within your agency's enterprise network, at a minimum, to prepare for and gain experience with the IPv6 protocol. This should not be considered a substitute for a full IPv6 transition effort that supports critical agency mission and function, but it will provide a baseline set of service for IPv6 architecture functionality, application testing, and experience/training of your personnel. A minimum set of actions you should take to establish the baseline includes:

- Establish an IPv6 test bed/pilot lab
- IPv6 addressing and routing plan
- Acquire IPv6 addresses
- Implement IPv6 security services (firewall, IDS, IPS, reporting)
- Enable required IPv6 services such as DNS and DHCPv6
- Enable IPv6 routing within the enterprise
- Establish external IPv6 connectivity (Internet, Internet2, DREN, other agencies)

For More Information visit **www.cisco.com/go/fedipv6**.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**