

---

# Planning Guide/Roadmap Toward IPv6 Adoption within the US Government

---

Version 1.0

May 2009



Architecture and Infrastructure Committee,  
Federal Chief Information Officers Council



**The Federal CIO Council Architecture and Infrastructure Committee  
Services Subcommittee & Governance Subcommittee**

**In collaboration with the**



**The American Council for Technology / Industry Advisory Council's  
Enterprise Architecture Shared Interest Group (EA-SIG)**

**Present:**

***Planning Guide/Roadmap Toward IPv6 Adoption within the US  
Government***

May 2009

# Table of Contents

|   |            |
|---|------------|
| <b>Intended Audience.....</b>                                     | <b>V</b>   |
| <b>Executive Summary.....</b>                                     | <b>vi</b>  |
| Our Business Situation.....                                       | vi         |
| The “To Be” State.....  | viii       |
| Required Action.....  | ix         |
| Contributors.....   | x          |
| <b>Section 1: Federal IPv6 Transition - Progress to Date.....</b> | <b>xii</b> |
| 1.1 OMB Memorandum M-05-22.....                                   | xii        |
| 1.2 IPv6-Enabled Infrastructures (Network Backbones).....         | xii        |
| 1.3 Harmonized Standards.....                                     | xii        |
| 1.3.1 US Government IPv6 Standards Profile.....                   | xii        |
| 1.3.2 IPv6 Test Program.....                                      | xiii       |
| 1.3.3 DoD IPv6 Profile.....                                       | xiii       |
| <b>Section 2: The Business Rationale for IPv6 .....</b>           | <b>15</b>  |
| <b>Section 3: Federal IPv6 Transition - The To Be State.....</b>  | <b>17</b>  |
| 3.1 IPv6-Enabled Network Services.....                            | 17         |
| 3.1.1 End-User Application Patterns.....                          | 17         |
| <b>Section 4: Leveraging Enterprise Architecture.....</b>         | <b>20</b>  |
| 4.1 Using the IT Infrastructure Segment Architecture.....         | 21         |
| 4.1.1 Developing a Service Oriented Infrastructure.....           | 23         |
| 4.2 EA Driven IPv6 Planning.....                                  | 23         |
| 4.2.1 Using the USG IPv6 Standards Profile.....                   | 25         |
| 4.3 Developing an IPv6 Transition Strategy Plan.....              | 29         |
| 4.4 Integration with Capital Planning.....                        | 30         |
| 4.5 OMB IPv6 EA Assessment Criteria.....                          | 31         |
| <b>Section 5: Transition Milestones.....</b>                      | <b>33</b>  |
| 5.1 Quick Wins.....   | 36         |
| 5.1.1 Establish an IPv6 Test Lab.....                             | 36         |
| 5.1.2 External Facing Servers.....                                | 37         |
| 5.2 IPv6 Network Service Deployment.....                          | 38         |
| 5.2.1 Develop Addressing and Routing Plan.....                    | 38         |
| 5.2.2 Address Acquisition.....                                    | 38         |
| 5.2.3 Establish Address Management and Allocation Procedures..... | 39         |
| 5.2.4 Domain Name Service (DNS) Assessment.....                   | 40         |
| 5.2.5 DHCPv6 Assessment.....                                      | 42         |
| 5.2.6 Network Management.....                                     | 43         |
| 5.2.7 Application Development.....                                | 44         |
| 5.2.8 IPv6 Desktop Access.....                                    | 45         |
| 5.3 Security .....  | 45         |
| 5.4 Additional Tips.....  | 48         |
| <b>Section 6: IPv6 Impact on Federal Initiatives.....</b>         | <b>50</b>  |
| 6.1 TIC51.....  | 50         |
| 6.2 HSPD-12.....  | 51         |
| 6.3 IT Infrastructure Line of Business (ITILoB).....              | 52         |
| 6.4 FDCC.....   | 52         |
| 6.5 Networx Migration.....  | 52         |
| 6.6 DNSSEC.....   | 53         |
| <b>Section 7: IPv6 in IT Governance and Procurement.....</b>      | <b>54</b>  |
| 7.1 Governance.....   | 54         |
| 7.2 Procurement.....  | 54         |

[Section 8: Acronym Dictionary.....56](#)  
[Appendix A: Guide to Incorporating IPv6 into IT Infrastructure  
Segment Architectures.....58](#)  
[References.....64](#)

## List of Tables

**Table 1 - IPv6 vs. IPv4 Features.....15**  
**Table 2 - IPv6 Capability Examples by LoB.....17**  
**Table 3 - Potential IPv6-Enabled Network Services.....24**  
**Table 4 - IPv6 Criteria in the Enterprise Architecture Assessment  
Framework v3.0.....32**

## List of Figures

**Figure 1 - Enterprise Architecture & Capital Planning IPv6 Roadmap  
.....ix**  
**Figure 2 - IPv6 Transition Concept of Operations.....20**  
**Figure 3 - Role of IT Infrastructure Optimization .....22**  
**Figure 4 - USGv6-V1 Capability Check List - Annex A.....28**  
**Figure 5 - Sample USG IPv6 Profile Excerpt.....29**  
**Figure 6 - FEA PMO’s Performance Improvement Lifecycle.....30**  
**Figure 7 - IPv6 Transition Phases and Timeline.....34**  
**Figure 8 - Proposed Timeline for IPv6 Transition.....35**  
**Figure 9 - IPv6 Relation to Other Federal Initiatives.....50**

## **Intended Audience**

This document is intended for chief information officers (CIOs), chief architects, and other individuals in federal agencies who are responsible for using information technology (IT) assets to assist in achieving the mission and objectives of the agency. The purpose of this document is to aid in understanding the Federal Government's Internet Protocol version 6 (IPv6) vision and to provide specific guidance for adopting this protocol. Based on the information in this document, the chief architect or CIO should be able to develop and explain a business case for IPv6 adoption, develop a Target Architecture and Transition Strategy Plan to guide the agency's IPv6 adoption, and integrate IPv6 requirements into impacted federal initiatives.

## Executive Summary

The purpose of this document is to provide U.S. government agency leaders with practical and actionable guidance on how to successfully integrate Internet Protocol version 6 (IPv6) throughout their enterprise. This guidance builds upon the Office of Management and Budget's previous requirement for agencies to prove IPv6 capability through core network infrastructure testing by June 30, 2008 (M-05-22) by providing:

1. Definition of the "To Be IPv6 State" of Federal IPv6 transition.
2. Overview of how to leverage Enterprise Architecture (EA) and Capital Planning and Investment Control (CPIC) to drive IPv6 transition.
3. Practical guidance and common milestones that agencies can use to facilitate deployment of IPv6-enabled network services in support of their core mission applications. Note: many custom mission applications that run on internal-only networks do not need to transition to IPv6.
4. Description of how IPv6 transition impacts other Federal initiatives, such as Trusted Internet Connections (TIC) and Homeland Security Presidential Directive (HSPD) -12.
5. Clear Positioning of IPv6 as an integrating framework and organizing principle for the next generation of Federal IT Infrastructure.

### Our Business Situation


Action is needed by the US Government in order to retain our nation's technical and market leadership in the Internet sector and to expand and improve

services for America's citizens. There has already been significant progress by foreign governments in attempting to reap the advantages of early IPv6 deployment, including the:

- China's Next Generation Internet project (CNGI), which is a five-year plan with the objective of cornering a significant proportion of the Internet space by implementing IPv6 early. China showcased CNGI and its IPv6 network infrastructure at the 2008 Olympics in Beijing, networking everything from security cameras and taxis, to the Olympic events cameras by using IPv6;
- European Commission's i2010 initiative, an action plan to see IPv6 widely deployed in Europe by 2010.<sup>1</sup>

IPv6 provides valuable benefits to agencies by facilitating an improvement in operational efficiencies and citizen services. Many of these benefits will not be realized until running IPv6 natively. Examples of IPv6 benefits include:

- **Addressing and Routing**  
IPv6's extremely large address space enables global connectivity to many more electronic devices – mobile phones, laptops, in-vehicle computers, televisions, cameras, building sensors, medical devices, etc.
- **Security**  
IPv6's security comes in the form of IPsec, which allows authentication, encryption, and integrity protection at the network layer.



*"IPv6 is a global undertaking and opportunity enabled by national and local strategies."*

**Latif Ladid,**  
IPv6 Forum President

- **Address Auto-Configuration**

IPv6 address auto-configuration enables simple devices to achieve out of the box plug-and-play network access that is key to self-organizing networks.

- **Support for Mobile Devices**

IPv6 enabled applications can benefit from seamless mobility. The mobility comes in the form of Mobile IPv6, which allows devices to roam among different networks without losing their network connectivity.

- **Peer-to-Peer (P2P) Communication Tools that Can Improve Interagency Collaboration**

True end-to-end connectivity, enabled by the IPv6 address space and elimination of private network addresses, will allow the optimization of media-streaming applications. This will enable timely video feeds and quality-rich information to be easily distributed to millions of locations.

IPv6 supports an integrated, well-architected platform for all the aforementioned benefits with headroom for future growth and enhancement.

***However, in order to realize the benefits offered by IPv6, it is important for the Federal Government to begin the process of architecting and deploying IPv6 enabled network services.***

***Based upon current forecasts by leading experts, the world's current allocation of IPv4 address spaces from the global pool will be exhausted by 2011-2012.*** As of September 2007, 4/5 of the world's IPv4 address space has been assigned, thereby leaving only 1/5 for future use.<sup>2</sup> Over the past five years, demand levels for addresses have been steadily accelerating due to rapid population growth, mass-market broadband deployment, the demand for globally unique addresses for applications such as *Voice over IP (VoIP)*, the addition of network addressable devices such as mobile phones and sensors to the Internet, and continuing real cost reductions in technology that has now brought the Internet to large populations in developing economies.

Demand for IP address space will also increase with the advent of ***cloud computing*** – which encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends IT's existing capabilities. One of the main advantages of IPv6 is that it re-establishes the P2P connection that was lost in IPv4 because of Network Address Translation (NAT) and cloud computing. IPv6 greatly simplifies the deployment of next generation services and the 'plug and play' experience.

***An Issue of Business Continuity***

*"The technical stuff for IPv6 is done. IPv6 is ready. This is a business issue in the internet service industry. The ISP community round the world needs to pay attention... They are persisting in the 'nobody is asking for this' mentality. They are not valuing business continuity as they should. When they finally wake up, there is going to be a mad scramble for IPv6 and they won't implement it properly".*

Vinton Cerf, September 30, 2008  
interview with "The Times Online".

**Vinton "Vint" Cerf is an American computer scientist who is the person most often called "the father of the Internet". His contributions have been recognized repeatedly, with honorary degrees and awards that include the National Medal of Technology, the Turing Award, and the Presidential Medal of Freedom.**

All of these factors contribute to an accelerating IPv4 address consumption rate. As a result, this has been the driving factor in creating and adopting several technologies, including classful networks, Classless Inter-Domain Routing (CIDR) addressing, Network Address Translation (NAT) and a new version of the Internet Protocol, IPv6.

The transition of the Internet to IPv6 is generally seen as the only practical and readily available long-term solution to IPv4 address exhaustion for devices connected to the public internet.

It should be recognized that by the end of 2011, there will be new clients and servers on the Internet which have no choice but to only have an IPv6 address (based on Internet Assigned Numbers Authority and American Registry for Internet Numbers warnings about the need for contiguous address assignment). For the rest of the Internet to be able to communicate with them they should then be able to: a) serve to IPv6 customers, and b) access IPv6 servers. Within scalable solutions, the first requires Internet-facing servers to be on IPv6, and the second requires almost all devices to be on IPv6. Non-public facing networks on private subnets or point-to-point leased lines that do not rely on carrier transport across the Internet core do not have a driver to migrate to IPv6 by 2012 and should migrate through gradual tech refresh.

To track the countdown to IPv4 Address Exhaustion, visit either [www.ipv6forum.com](http://www.ipv6forum.com) or <http://penrose.uk6x.com/>.

This development has caused the American Registry for Internet Numbers (ARIN) to unanimously pass a resolution encouraging the Internet community to begin migration to IPv6 numbering resources where possible (see <http://www.arin.net/v6/v6-resolution.html>).

Therefore, without a concentrated effort by Federal agencies to effectively and efficiently deploy IPv6 network services, the Government's technical advancement and ability to meet its mission needs will be critically impacted during the next 2 to 3 years. The exhaustion of IPv4 address space will prevent:

- The US Government from providing new Internet-based services enhancing/expanding existing Internet-based services since new hosts will not be able to connect to the Internet;
- Internet connection providers from increasing the number of their subscribers.

### **The “To Be” State**

*The deployment of secure, end-to-end, IPv6-enabled network services which support federal agency core missions and applications.*

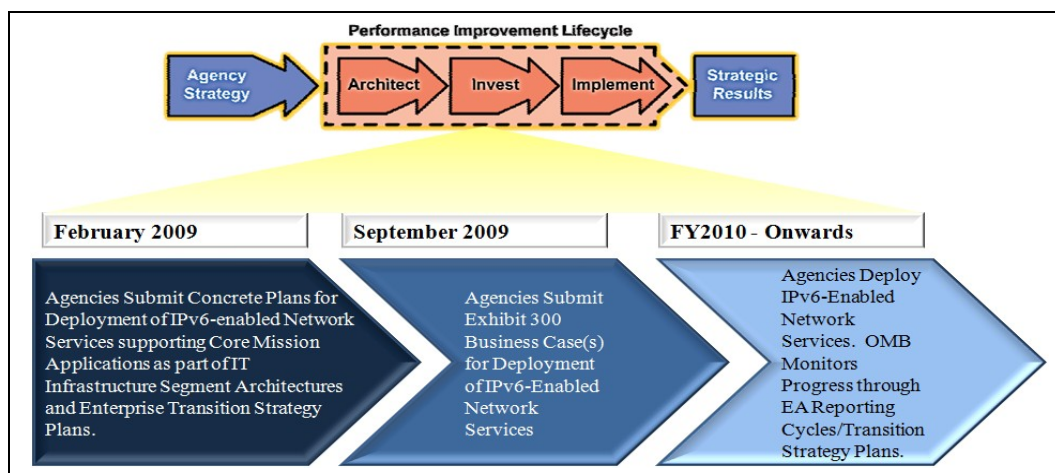
OMB has stated that all departments and agencies met the deadline to report successful demonstration of IPv6 capability by June 30, 2008. According to OMB, “agencies should focus on establishing secure, shared IPv6-enabled network services during their regular technology upgrade cycles. They should also use their enterprise architecture and capital planning activities to prepare for that.”<sup>3</sup> In addition, OMB states that “agencies are expected to be including IPv6 in their enterprise architecture plans and OMB is updating its Enterprise Architecture Assessment Framework to address transition strategies and investment proposals. It has to be business case driven.”<sup>4</sup> Like other areas of strategic investment which lead to new levels of productivity, greater mission successes and citizen access to government, IPv6 integration must be prioritized at the agency level and executed in a well planned, phased approach with success criteria

measurements and alignment with other key government initiatives like TIC, HSPD-12, FDCC, NETWORX, DNSSEC and the IT Infrastructure Line of Business (ITI LoB). To open the door for new forms of collaboration within government, new forms of information sharing and gathering, and new citizen services and access, it is critical for agency leaders to continue with the integration of IPv6 into their infrastructures and across their enterprise networks. IPv6 integration is an accelerator to the establishment of a Service Oriented Infrastructure (SOI), which is a collection of functioning capabilities that enable safe and efficient collaboration through the development and deployment of shared operational IT services.

### **Required Action**

As we move forward, integration of IPv6 and the creation of dual-stacked (IPv4 and IPv6) protocol environments should not be taken lightly. IPv6 has horizontal reach across an agency’s enterprise environment; therefore a key to successful integration is a phased approach that results in a transition plan for all users, network-connected servers, applications, appliances and elements. IPv6 should be incorporated into agency IT Infrastructure Segment Architectures, tying network services to core mission segment architectures.

For this reason, agencies are advised to adopt and follow an Enterprise Architecture (EA) strategy similar to OMB’s EA concept: “Architect-Invest-Implement”.



**Figure 1 – Enterprise Architecture & Capital Planning IPv6 Roadmap**

Each lifecycle phase is comprised of tightly integrated processes that combine to transform the agency’s top-down strategic goals and bottom-up system needs into a logical series of work products designed to help the agency achieve strategic results. This approach provides a high-level EA-driven concept timeline which illustrates the integration of EA with Capital Planning and Investment Control – leading directly into the execution of IPv6-related projects. IPv6 should be reflected in agency IT Infrastructure Segment Architectures and Transition Strategy Plans, tying network services to core mission segment architectures. To ensure that a successful IPv6 transition plan is developed, funded, and executed, it is recommended that agencies adopt and follow this approach and timeline to align agency planning efforts with OMB EA expectations and strategies.

## Contributors

This document was produced by a team of dedicated individuals led by the Federal IPv6 Working Group of the Technology Infrastructure Sub-Committee (TIS). The TIS is a formally chartered sub-organization of the Architecture and Infrastructure Committee (AIC) of the Federal Chief Information Officer (CIO) Council. The Clinger-Cohen Act of 1996 authorizes the Federal CIO Council. This guide was developed in conjunction with the American Council for Technology/Industry Advisory Council.

The following AIC leadership members were responsible for the development of this guide:

| Name             | Role                             | Title                                       | Organization         |
|------------------|----------------------------------|---|----------------------|
| Molly O'Neill    | AIC Co-Chair                     | CIO   | EPA                  |
| Michael Carleton | AIC Co-Chair                     | CIO   | HHS                  |
| Cita Furlani     | TIS Co-Chair                     | Director, Information Technology Laboratory | NIST                 |
| Bobbie Stempfley | TIS Co-Chair                     | DISA Deputy CIO                             | DoD                  |
| Peter Tseronis   | Federal IPv6 Working Group Chair | Deputy Associate Chief Information Officer  | Department of Energy |

The following persons were primary contributors to developing this guide:

| Name               | Role            | Title   | Organization   |
|--------------------|-----------------|---|--|
| Kshemendra Paul    | Editorial Board | Chief Architect                                 | OMB  |
| John Curran        | Editorial Board | Chairman, American Registry of Internet Numbers | (EVP, COO & CTO, ServerVault Corp)   |
| Jim Bound          | Editorial Board | CTO, IPv6 Forum                                 | (Chair North American IPv6 Task Force (NAv6TF): HP Senior Fellow)                                |
| Yanick Pouffary    | Editorial Board | IPv6 Forum Fellow                               | (North American IPv6 Task Force Technology Director; HP Distinguished Technologist)              |
| Tony Hain          | Editorial Board | IPv6 Forum Fellow                               | (NAv6tf Technical Director; Cisco Systems Technical Leader)                                      |
| Trey Hodgkins, CAE | Editorial Board | Vice President                                  | (Federal Government Programs Public Sector Group, Information Technology Association of America) |
| Brett Thorson      | Editorial Board | Network Integration & Security Advisor          | (North American IPv6 Task Force Network & Infrastructure Specialist – Boeing)                    |

## Planning Guide/Roadmap Toward IPv6 Adoption within the US Government

| Name                | Role                                    | Title  | Organization          |
|---------------------|---|--|-----------------------|
| Branko Primetica    | Key Contributor/<br>Project Coordinator | Vice President   | (eGlobalTech)         |
| David Rubal         | Key Contributor                         | Regional Manager, Federal<br>Unified Communications        | (Cisco)               |
| David Green         | Key Contributor                         | Vice President R&D   | (CommandInformation)  |
| Dale Geesey         | Key Contributor                         | Chief Operating Officer                                    | (Auspex Technologies) |
| Dr. Chuck Lynch     | Key Contributor                         | Chief: Data, Tools &<br>Analysis (DTA)                     | NIH                   |
| Doug Montgomery     | Key Contributor                         | Manager, Internetworking<br>Technologies Research<br>Group | NIST                  |
| Terry Sullivan      | Key Contributor                         | Business Development<br>Director                           | (BT Federal)          |
| Tim Rooney          | Key Contributor                         | Director, Product<br>Management                            | (BT Diamond IP)       |
| John Zuena          | Key Contributor                         | Sr. Network Engineer                                       | (BT Federal)          |
| Dokmai Webster      | Key Contributor                         | President  | (PivotalPoint)        |
| Ralph Wallace       | Key Contributor                         |  | (CommandInformation)  |
| Stephen Nightingale | Key Contributor                         |  | NIST                  |
| James McCabe        | Key Contributor                         | Network Architect  | Independent Advisor   |
| Lesley Skorupski    | Editor                                  | Technical Writer   | (eGlobalTech)         |

In addition, the following individuals supported the development of this document.

| Name               | Organization                                      |
|--------------------|---|
| Vivek Bajpai       | Unisys (OMB FEA PMO Support Contractor)           |
| Eugene Sokolowski  | GSA   |
| Frederick Schobert | GSA   |
| Gerald Lepisko     | IRS   |
| Rick Shew          | VA  |
| Susan Hotzler      | VA  |
| Carol Bales        | OMB   |
| Kris Strance       | DoD   |
| Ralph Liguori      | DoD   |
| Steven Pirzchalski | VA  |
| Tony Zanfordino    | VeriSolv Technologies Inc (VA Support Contractor) |
| Everett Dowd       | DoT   |
| John Baird         | DoD - Defense Research and Engineering Network    |

If you contributed to this effort and do not see yourself listed, your efforts were appreciated and we would like to recognize them here. Please help us correct any oversights by sending an email to [branko.primetica@eglobaltech.com](mailto:branko.primetica@eglobaltech.com).

# **Section 1: Federal IPv6 Transition - Progress to Date**

The discussion of IPv6 in the US Government has been active since 2003. Early initiatives led by the US Department of Defense (DoD) and the Office of Management and Budget (OMB) stakeholders drove agencies to demonstrate progress in areas of standardization and testing/certification to prepare for eventual government-wide IPv6 integration and transition. As of July 2008, all major agencies met the June 30, 2008 deadline for successfully demonstrating their adoption of IPv6 technology.

As the result of these efforts, it is important to understand the various IPv6 transition initiatives undertaken in federal government, where they currently stand, and how they can be leveraged in your successful transition plan.

## **1.1 OMB Memorandum M-05-22**

Dated August 2<sup>nd</sup> 2005, OMB Memorandum M-05-22 laid the groundwork for the early stages of integration by requiring United States Government (USG) agencies to prove IPv6 capability over IP backbone networks through basic testing, certification, and reporting by June 30, 2008. The memo was broadly seen by government and industry as the critical timeline in which IPv6 readiness had to be satisfactorily demonstrated across the Federal government.

A copy of the OMB Memorandum M-05-22 is available online at [www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf](http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf).

## **1.2 IPv6-Enabled Infrastructures (Network Backbones)**

On June 30<sup>th</sup> 2008, OMB released a public statement indicating that all major USG agencies met the M-05-22 deadline, reporting successful demonstration of IPv6 capability resulting in “IPv6-enabled network backbones”. Agencies were encouraged to move forward with IPv6 integration as part of their Enterprise Architecture planning and with IPv6-enabled backbone networks, agencies could begin the process of planning for phased integration of applications and users in a dual-stacked environment (IPv4 and IPv6 co-existing in the same network).

## **1.3 Harmonized Standards**

### **1.3.1 US Government IPv6 Standards Profile**

OMB Memorandum M-05-22 also directed the National Institute of Standards and Technology (NIST) to develop the technical infrastructure (standards and testing) necessary to support wide scale adoption of IPv6 in the USG. In response, NIST developed a technical standards profile for US Government acquisition of IPv6 hosts and routers and a specification for network protection devices. The Host and Router Profile includes a forward looking set of Requests for Comments (RFC's) published by the Internet Engineering Task Force (IETF), encompassing basic IPv6 functionality, and specific requirements and key optional capabilities for routing, security, multicasting, mobility, network management, and quality of service. The Network

Protection Device profile contains a NIST established set of capability requirements for IPv6 aware firewalls and intrusion detection systems.<sup>5</sup>

This Profile, which can be found at <http://www.antd.nist.gov/usgv6/profile.html>, underwent extensive vetting by both industry and the Federal IT community. It lists the Federal technical requirements for secure and inter-operable network products into the global IPv6 marketplace.

### 1.3.2 IPv6 Test Program

Following publication of the USG IPv6 Standards Profile, an infrastructure to demonstrate IPv6 product compliance needed to be set up. As a result, NIST is establishing a testing program based on ISO 17025 accredited test laboratories and standard reference tests, to assure compliance of Hosts, Routers and Network Protection Devices.

NIST is developing a document SP 500-273 Guidance on IPv6 Test Methods and Validation. This is pre-requisite to open public review of the test specifications, and Accreditation Bodies' establishing assessment programs, leading to the creation of Test Laboratories that adhere to the ISO 17025 "General Requirements for the Competence of Testing and Calibration Laboratories".

The goal is to have USG compliant IPv6 devices available for acquisition by July 2010. Compliance is signaled by device vendors issuing a "Suppliers Declaration of Conformance", based on ISO 17050. Specific provisions of this SDOC require that host and router products be tested for conformance and interoperability, and network protection products undergo functional testing, in accredited laboratories.

### 1.3.3 DoD IPv6 Profile

A Memorandum issued by the Assistant Secretary of Defense – Networks and Information Integration (ASD(NII)) entitled “DoD Internet Protocol Version 6 (IPv6) Definitions” in June 2008 updated the definition of “IPv6 Capable Products” and “IPv6 Capable Networks” in the context of products intended for use in Department of Defense (DoD) networks. IPv6 Capable Products shall be able to interoperate with other IPv6 Capable Products on networks supporting only IPv4, only IPv6, or both IPv4 and IPv6. In addition these products are to be conformant with the IPv6 standards contained in the DoD IT Standards Registry (DISR) as elaborated in “The DoD IPv6 Standards Profiles for IPv6 Capable Products.” The first version of the DoD IPv6 Profile was published in July 2006, and it has been updated annually. The current officially promulgated version is Version 3.0, published in June 2008 and available at: [http://jitc.fhu.disa.mil/apl/ipv6/pdf/dsr\\_ipv6\\_product\\_profile\\_v3.pdf](http://jitc.fhu.disa.mil/apl/ipv6/pdf/dsr_ipv6_product_profile_v3.pdf).

The DoD IPv6 Profile provides guidance on applying DoD policy, DoD Information Standards Registry (DISR) requirements, DoD IPv6 Transition Office (DITO) guidance, and IETF requirements to clearly define the requirements for IPv6 Capable networking equipment for acquisitions. The DoD IPv6 Profile defines specific tailored standards profiles for six product classes (Host/Workstation, Router, Layer 3 Switch, Network Appliance/Simple Server, Security Device, and Advanced Server) by identifying the standards (RFCs) that apply to products of that class.

The DoD IPv6 Profile lists each standard according to its level of requirement:

- **MUST:** The standard is required to be implemented in the product now, it is essential to IPv6 capability and interoperability.

- **SHOULD:** The standard is strongly recommended and should be followed in implementation unless there are particular circumstances justifying its omission.
- **SHOULD+:** Similar to SHOULD, however the standard will likely advance to **MUST** in the next version of the DoD IPv6 Profile or on a specific timeline identified in the text.
- **Conditional Requirement:** a requirement at one of the above levels is only called for in particular application or deployment.

While the USG IPv6 Profile (developed by NIST) and the DoD IPv6 Profile started as independent efforts, the current published versions reflect collaboration between the editorial teams to harmonize the two documents. Most of the differences between the earlier versions have been harmonized, and the residual differences reflect specific mission requirements particular to target users of each document. For example, the DoD Profile mandates the use of the Suite-B encryption algorithms [RFC 4869] based on DoD policy; however, these algorithms are considered beyond current civilian requirements.

The editors of the two Profiles agree that the documents need not be identical, but are now compatible, in that commercial products certified to meet either are unlikely to have interoperability issues with products certified to meet the other. The two editorial teams will continue to dialog and cross-review to maintain compatibility through future updates.

## Section 2:

# The Business Rationale for IPv6

The robustness, scalability, and limited feature set of IPv4 is currently being tested by a consistently expanding need for new IP addresses. This need is being spurred in large part by the rapid growth of:

- New network-aware devices, such as cellular phones;
- IP-based services, such as Voice over Internet Protocol (VoIP);
- The move toward a ubiquitously connected society.

The ability to integrate computers with everyday devices such as mobile phones, handheld devices, and home entertainment, is a key factor in the move towards a connected society and improved business efficiency. Federal Government personnel and information workers need integrated, secure functionality that helps them manage their professional lives: e-mail, instant messaging (IM), contact management, shared calendars, and relationship management.

IPv4 is not capable of enabling a connected society and meeting the government’s business needs due to limited address space and features. In fact, the Department of Defense (DoD) issued a memorandum on June 9, 2003 stating that “IPv4 is incapable of meeting the long-term requirements of the commercial community and the DoD. IPv6 is designed to overcome those limitations.”

The table below provides a high level business-focused summary of the advantages IPv6 has over IPv4 in terms of features.

**Table 1 – IPv6 vs. IPv4 Features**

| Feature                                | IPv6  | IPv4  |
|--|---|---|
| <b>Easier management of networks</b>   | IPv6 networks provide autoconfiguration capabilities. They are simpler, flatter and more manageable, especially for large installations.  | Networks must be configured manually or with Dynamic Host Configuration Protocol (DHCP). IPv4 has had many overlays to handle Internet growth, which demand increasing maintenance efforts. |
| <b>End-to-end connective integrity</b> | Direct addressing is possible due to vast address space - the need for network address translation devices is effectively eliminated. This allows network resources to have their own unique real IP addresses, | Widespread use of Network Address Translation (NAT) devices means that a single NAT address can mask thousands of non-routable addresses, making end-to-end integrity unachievable.         |

*“..the FAA, Department of Commerce, the Department of Homeland Security, and the rest of these guys must sooner or later mandate it [IPv6] as well because you can't have one network in a federal government that can't work with the networks [from other countries], such as Japan, China, Europe, South Korea, or even the United Nations, which have all [backed] IPv6.”*

**Alex Lightman**  
**Founding CEO and Chairman of IPv6 Summit, Inc.**

| Feature   | IPv6  | IPv4  |
|---|---|---|
|   | paving the way for secure end-to-end peer-to-peer networks. This will enable people to access information and share resources without going through a complex maze of middle boxes that requires IT management. |   |
| <b>Unconstrained address abundance</b>                          | $3.4 \times 10^{38} = 340$ trillion trillion trillion addresses - about 670 quadrillion addresses per square millimeter of the Earth's surface.   | $4.29 \times 10^9 = 4.2$ billion addresses - far less than even a single IP address per person on the planet.                         |
| <b>Platform for innovation, collaboration, and transparency</b> | Given the numbers of addresses, scalability and flexibility of IPv6, its potential for triggering innovation and assisting collaboration is unbounded.  | IPv4 was designed as a transport and communications medium, and increasingly any work on IPv4 is to find ways around the constraints. |
| <b>Integrated interoperability and mobility</b>                 | IPv6 provides interoperability and mobility capabilities which are already widely embedded in network devices.  | Relatively constrained network topologies restrict mobility and interoperability capabilities in the IPv4 Internet.                   |
| <b>Improved security features</b>                               | IPSEC is built into the IPv6 protocol, usable with a suitable key infrastructure.   | Security is dependent on applications - IPv4 was not designed with security in mind.  |

Although there is an increasing sense of urgency in Federal Government to start moving toward IPv6, it is not the same situation as Y2K, which had a clear date by which transition was vital. New allocation policies for both IPv4 and IPv6 addresses have been drawn up, and discussion is ongoing about how best to reintroduce unused IP addresses into the system. It is important to note, however, that the transition to IPv6 is more complex than previous advances in Internet technology (from dial-up modems to always-on DSL or from host files to the domain name system). This critical step toward the “Next Generation Internet” requires immediate attention and detailed planning for success.

## Section 3:

# Federal IPv6 Transition - The To

*"Transitioning to IPv6 is a critical journey that must begin today for the U.S. Government and Industry before the exhaustion of the current IPv4 address space, to assist with the restoration of the Internet End-2-End model, and an important technical optimization for Next Generation Networks technology such as Voice Over IP (VOIP), Always Connected Seamless Network Mobility, IPTV, and Cloud services for ubiquitous mobile devices."*

**Jim Bound,  
CTO, IPv6 Forum Chair North  
American IPv6 Task Force  
(NAv6TF)**

## Be State

The next step in the Federal IPv6 transition is the deployment of secure, end-to-end, IPv6-enabled network services which support Federal Agency Core Missions and applications - from the core to the server center and to desktop and mobile platforms. This will be accomplished by upgrading, piloting and launching entire production subnets with IPv6 applications and desktop/mobile services. The Internet Protocol upgrade is a core technology that must be addressed in programs of record when purchasing solutions such as unified communications, workgroup collaboration tools, web-applications and other end-user applications.

### 3.1 IPv6-Enabled Network Services

This section contains examples of common network services that are candidates for IPv6-enablement. Additional examples can be found in Table 3.

#### 3.1.1 End-User Application Patterns

IPv4 address exhaustion will eventually break the ability to communicate effectively across the Internet core in IPv4 - making IPv6 a necessary upgrade for applications that communicate across the Internet. The following table provides high-level examples of IPv6 features and capability enhancements that could be deployed, by Line of Business (LoB), throughout the federal community:

**Table 2 – IPv6 Capability Examples by LoB**

| Line of Business                               | Objectives / Requirements   | IPv6 Feature and Capability Enhancements   |
|--|---|--|
| <b>Land Use, Mapping, and Agriculture</b>      | <ul style="list-style-type: none"> <li>• Resource tracking and allocation via sensor networks</li> <li>• Land boundary and border marking via tags with IP addresses</li> </ul>   | <ul style="list-style-type: none"> <li>• Ad-hoc routing via neighbor discovery</li> <li>• Address tagging with low-order 64-bit identifiers</li> <li>• Extension headers (location-based services)</li> <li>• Unified Communications</li> <li>• Mobile Applications Access</li> <li>• Teleworking/Distributed Workforce</li> <li>• Sensor Networks</li> </ul>  |
| <b>Science, Green Science, and Weather</b>     | <ul style="list-style-type: none"> <li>• Improved utilization of existing infrastructure</li> <li>• Sensor networking</li> </ul>  | <ul style="list-style-type: none"> <li>• Satellite communications</li> <li>• Ad-hoc routing via neighbor discovery</li> <li>• Extension headers (location-based services)</li> <li>• Unified Communications</li> <li>• Mobile Applications Access</li> <li>• Teleworking/Distributed Workforce</li> <li>• Sensor Networks</li> </ul>   |
| <b>Commerce, Banking, and Finance</b>          | <ul style="list-style-type: none"> <li>• End-to-end network security authentication and encryption</li> </ul>   | <ul style="list-style-type: none"> <li>• IPSec authentication and encryption</li> <li>• Extension headers (financial attributes)</li> <li>• Unified Communications</li> </ul>  |
| <b>Information Science and IT Optimization</b> | <ul style="list-style-type: none"> <li>• Streamlined data flows and reduced networking complexity</li> <li>• Improved end-to-end multimedia and converged communications</li> <li>• Virtual services and tele-presence</li> </ul> | <ul style="list-style-type: none"> <li>• Flow labels for priority data flows</li> <li>• Optimized hierarchical addressing and routing</li> <li>• Extension headers (variable)</li> <li>• Unified Communications</li> <li>• Teleworking/Distributed Workforce</li> </ul>  |
| <b>Justice and Law Enforcement</b>             | <ul style="list-style-type: none"> <li>• Asset deployment identification and tracking</li> <li>• Real-time, ad-hoc, interoperable communications</li> </ul>   | <ul style="list-style-type: none"> <li>• Address tagging with low-order 64-bit identifiers</li> <li>• Mobile, ad-hoc routing via neighbor discovery</li> <li>• Unified Communications</li> <li>• Mobile Applications Access</li> <li>• Teleworking/Distributed Workforce</li> <li>• Asset Tracking/ITV</li> </ul>  |
| <b>Privacy, Protection, and Security</b>       | <ul style="list-style-type: none"> <li>• Mandatory, end-to-end authentication and encryption</li> <li>• Non-attributable addresses</li> </ul>   | <ul style="list-style-type: none"> <li>• IPSec authentication and encryption</li> <li>• Extensive address pool</li> <li>• Unified Communications</li> </ul>  |
| <b>Homeland Protection and First Response</b>  | <ul style="list-style-type: none"> <li>• Secure communications</li> <li>• Mobile, ad-hoc communications for first responders</li> <li>• Total force and asset integration</li> </ul>  | <ul style="list-style-type: none"> <li>• IPSec authentication and encryption</li> <li>• Mobile, ad-hoc routing via neighbor discovery</li> <li>• Address tagging with low-order 64-bit identifiers</li> <li>• Unified Communications</li> <li>• Mobile Applications Access</li> <li>• Teleworking/Distributed Workforce</li> <li>• Sensor Networks</li> <li>• Transportation Automation (Wireless Access in Vehicle Environments)</li> </ul> |

| Line of Business  | Objectives / Requirements  | IPv6 Feature and Capability Enhancements  |
|---|--|---|
| <b>Defense, Intelligence, and Military Operations</b>                 | <ul style="list-style-type: none"> <li>• Secure, mobile communications</li> <li>• Mobile, ad-hoc communications for war fighters</li> <li>• Asset integration and insightful logistics</li> <li>• Military Training/Mission Rehearsal</li> </ul> | <ul style="list-style-type: none"> <li>• IPSec authentication and encryption</li> <li>• Mobile, ad-hoc routing via neighbor discovery</li> <li>• Address tagging with low-order 64-bit identifiers</li> <li>• Extension headers (specialize, private use)</li> <li>• Unified Communications</li> <li>• Mobile Applications Access</li> <li>• Teleworking/Distributed Workforce</li> <li>• Asset Tracking/ITV</li> <li>• RFID</li> <li>• Sensor Networks</li> <li>• Transportation Automation (Wireless Access in Vehicle Environments)</li> </ul> |
| <b>Education, Learning, Knowledge Management, and Library Science</b> | <ul style="list-style-type: none"> <li>• Improved end-to-end multimedia and converged communications</li> <li>• Virtual services and tele-presence</li> </ul>  | <ul style="list-style-type: none"> <li>• Flow labels for priority data flows</li> <li>• Source routing for more efficient transport</li> <li>• Unified Communications</li> <li>• Teleworking/Distributed Workforce</li> <li>• Mobile Applications Access</li> </ul>   |
| <b>Transportation Optimization, Shipping, and Tracking</b>            | <ul style="list-style-type: none"> <li>• Transport and container tracking via sensor networks</li> <li>• Live traffic reporting and communications</li> </ul>  | <ul style="list-style-type: none"> <li>• Ad-hoc routing via neighbor discovery</li> <li>• Address tagging with low-order 64-bit identifiers</li> <li>• Unified Communications</li> <li>• Mobile Applications Access</li> <li>• Teleworking/Distributed Workforce</li> <li>• Asset Tracking/ITV</li> <li>• RFID</li> <li>• Sensor Networks</li> </ul>  |
| <b>Health and Biomedical Science</b>                                  | <ul style="list-style-type: none"> <li>• Tele-presence</li> <li>• Tele-science (real-time)</li> <li>• Records management and security</li> </ul>   | <ul style="list-style-type: none"> <li>• Flow labels for priority data flows</li> <li>• Extension headers (attribution characteristics)</li> <li>• IPSec authentication and encryption</li> <li>• Unified Communications</li> <li>• Mobile Applications Access</li> <li>• Teleworking/Distributed Workforce</li> </ul>  |
| <b>Constituent Services (Delivery and Tracking)</b>                   | <ul style="list-style-type: none"> <li>• Tracking via sensor networks</li> <li>• Package locations services</li> </ul>   | <ul style="list-style-type: none"> <li>• Ad-hoc routing via neighbor discovery</li> <li>• Address tagging with low-order 64-bit identifiers</li> <li>• Extension headers (Location-based services)</li> <li>• Sensor Networks</li> <li>• Asset Tracking/ITV</li> </ul>  |

## Section 4:

# Leveraging Enterprise Architecture

The purpose of this section is to describe how to use the Enterprise Architecture (EA) and the IT Infrastructure Segment Architecture as a strategic planning and execution tool to enable effective IPv6 deployment. The architectures should be used to:

1. Assess the “As-Is” IPv4 and IPv6 environments;
2. Envision your agency’s “To-Be” IPv6 state, defining network services to be IPv6-enabled based upon the agency’s business needs;
3. Develop an IPv6 Transition Strategy to address the gaps between the “As-Is” and “To-Be” IPv6 environments;
4. Invest in IPv6-enabled network services (as defined in your Target Enterprise Architecture) through the Capital Planning and Investment Control (CPIC) process;
5. Monitor IPv6 deployment progress according to the milestones defined in your agency’s Transition Strategy Plan.

This concept of operations and the relationship between EA and CPIC is illustrated below.

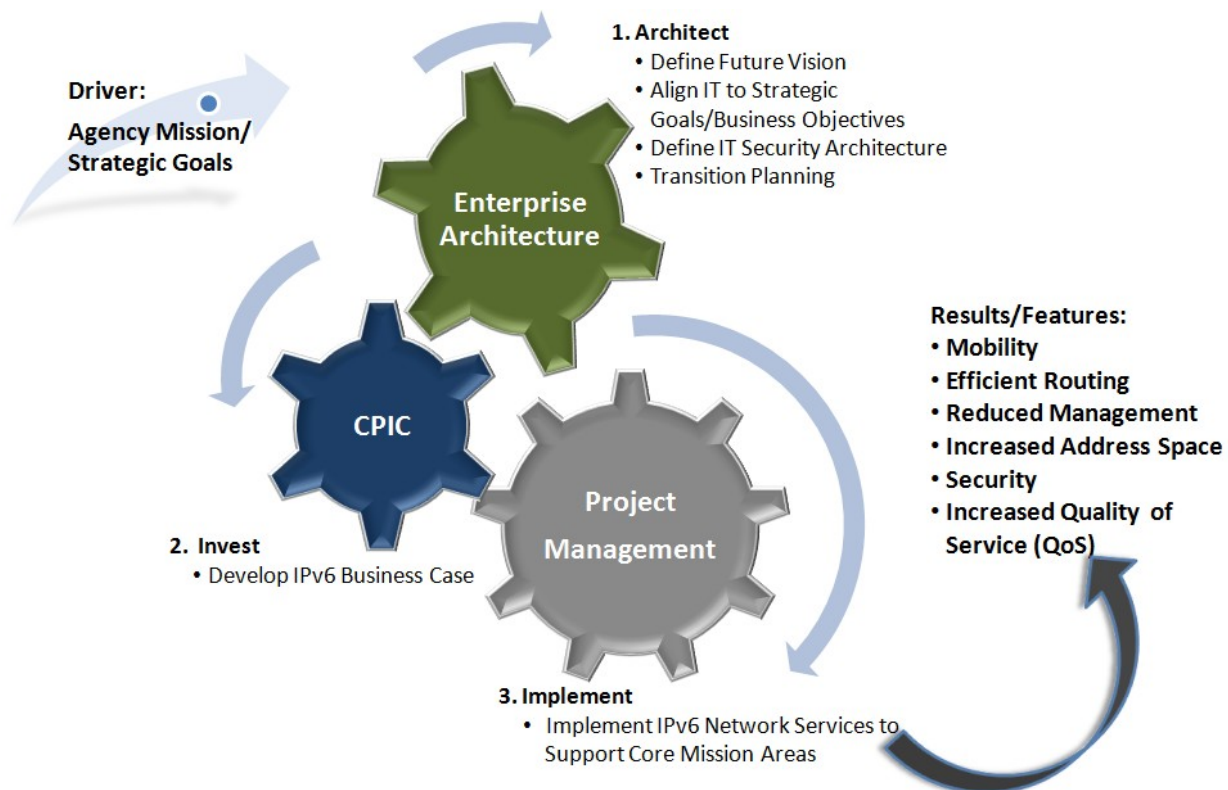


Figure 2 – IPv6 Transition Concept of Operations

The OMB Federal Enterprise Architecture Program Management Office (FEA PMO) will monitor Government-wide IPv6 transition progress through the following reporting mechanisms:

- **Annual Enterprise Architecture Assessment:** Federal Agencies are required to submit their completed Segment Architectures, using the reporting templates defined by the Federal Segment Architecture Methodology (FSAM), at the end of each February. Thereafter, agencies will be required to submit updated Segment Architecture submissions each quarter so that OMB can assess Segment Architecture progress.

Additionally, The OMB EA reporting and assessment cycle has been modified to further tighten alignment of EA with agency strategic planning and mission performance improvement, capital planning and investment control (CPIC), and results reporting:

- Quarterly milestone reporting – Starting in February 2009, agencies will submit a completed reporting template for each agency-defined segment.
- Annual status assessment – Starting in the FY 09 cycle, OMB will assess “Completion” in the 3<sup>rd</sup> fiscal quarter; assess “Use” in the 4th fiscal quarter; and assess “Results” in the 1st fiscal quarter.

Therefore, agencies will need to incorporate IPv6 modernization activities into their IT Infrastructure Segment Architecture reporting template (as provided through the Federal Segment Architecture Methodology) starting in February 2009. Subsequently, agencies will be assessed on IPv6 transition progress each 3<sup>rd</sup> fiscal quarter (IPv6 falls under the “Completion” capability under the OMB EAAF Version 3.0).

OMB assessment scores are incorporated into each agency’s President’s Management Agenda Scorecard.

## 4.1 Using the IT Infrastructure Segment Architecture

OMB will require agencies to incorporate IPv6 modernization activities into their IT Infrastructure Segment Architectures, which should be aligned to the Federal Transition Framework (FTF). The FTF is a single information source for cross-agency information technology (IT) initiatives, found at <http://www.whitehouse.gov/omb/e-gov/fea/>.

The rationale behind this requirement is that agency IT Infrastructures provide network services and support core mission applications, as illustrated in Figure 3.

The Federal IT Infrastructure Program Management Office (ITI PMO) will issue guidance on how to develop IT Infrastructure Segment Architectures. The ITI PMO, supporting the Federal IT Infrastructure Line of Business (ITI LoB), seeks to identify opportunities for IT infrastructure consolidation and optimization, and develop government-wide common solutions. The scope is all Federal IT commodity services including:

- Data Centers
- Data Networks and Telecommunications
- Desktop / Seat Management and Support

Agencies should integrate their IPv6 target visions into the following layers of their IT environment, as appropriate:

- **Business Architecture:** Refers to capabilities or tasks that enable the achievement of agency mission objectives. Core business functions will be supported or enhanced by IPv6-enabled services. As a reference point, consider earlier the introduction of

telephones and the Internet as examples of infrastructure-enabled business function transformations.

- **Application Architecture:** Refers to components/applications that enable the business needs and services defined in the Business Architecture.
  - Application development and certification processes must ensure that IPv6 is supported
  - Development environments, service-oriented architecture (SOA), and Web services, should be updated to include IPv6
- **Technology Architecture:** Refers to assets that support IT services and communications. IPv6 migration goes beyond network backbone upgrades to:
  - Basic naming services, such as DNS and DHCP
  - Common shared infrastructure services, such as file, print, database, and Web services
  - Individual computing units.

A guide, or template, for incorporating IPv6 modernization activities into all layers of an agency's IT infrastructure segment architecture can be found in Appendix A. This template should be used as high-level guidance and is not a requirement.

The following graphic depicts the critical underlying role that IT infrastructure optimization and related initiatives play in improving agency and program performance to provide better services to end customers and the impact that IPv6 has in realizing these benefits.

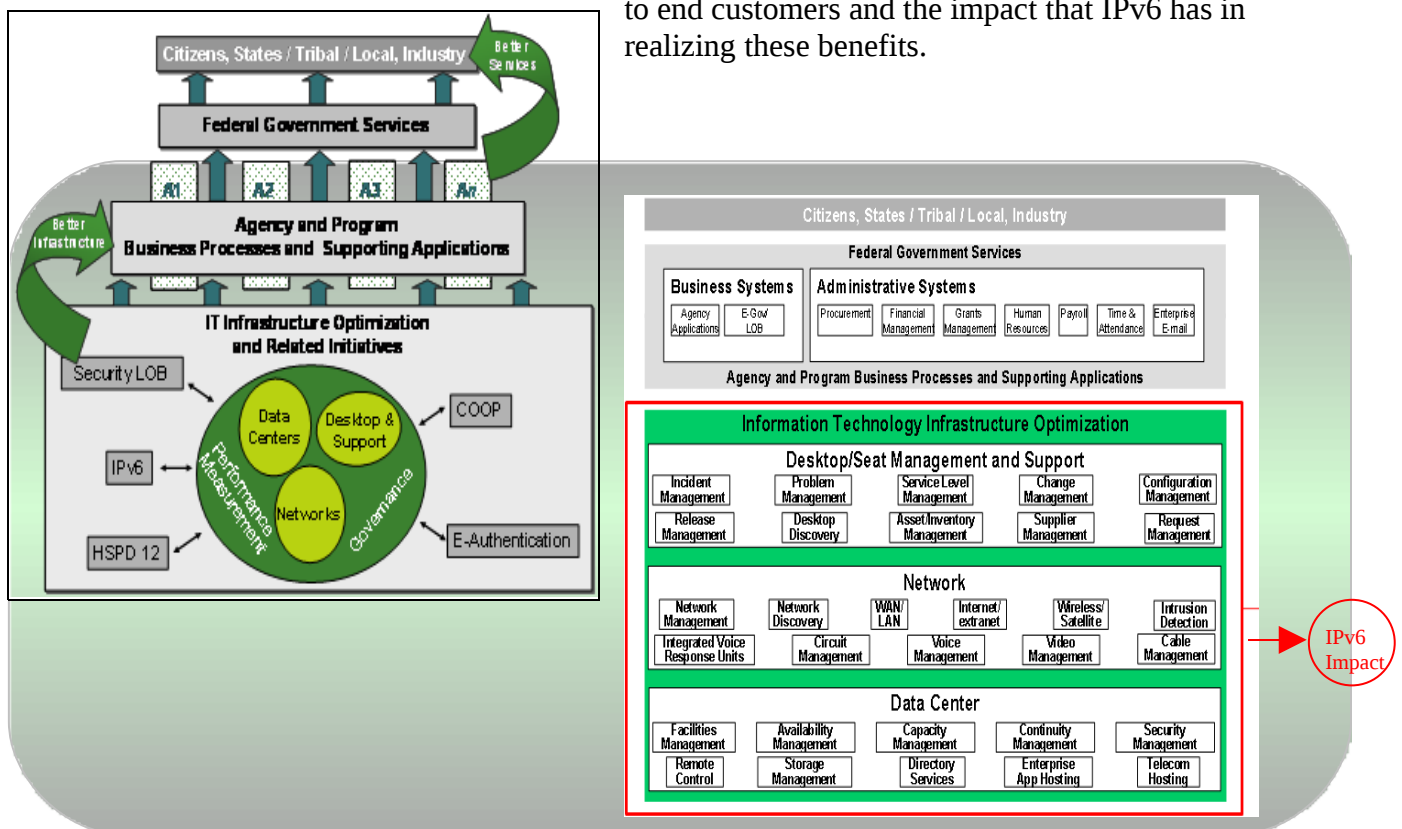


Figure 3 – Role of IT Infrastructure Optimization

### 4.1.1 Developing a Service Oriented Infrastructure

Service Oriented Infrastructure (SOI) is a framework for delivering core infrastructure services as a “service” to the business rather than individual components. SOI can also be defined as a collection of functioning capabilities, including technology, standards, and collaborative processes that enable safe and efficient collaboration through the development and deployment of shared operational IT services. A key aspect of SOI is providing IT Infrastructure services via a pool of resources (web servers, application servers, database servers, servers, storage instances) instead of through discrete instances.<sup>6</sup> The term SOI also has a broader usage, which includes all configurable infrastructure resources such as compute, storage, and networking hardware and software to support the running of applications.<sup>7</sup> Consistent with the objectives for Service Oriented Architecture (SOA), SOI facilitates the reuse and dynamic allocation of necessary infrastructure resources. The development of SOI solutions focuses around the service characteristics to be provided, which are the basis for both the development and the delivery of services.

*At DOT, IPv6 can provide the infrastructure for services developed with the Intelligent Transportation Systems (ITS), the Vehicle Infrastructure Integration Project, and the Next Generation Air Transportation System (Next Gen).*

IPv6 provides significant advantages in the deployment of a SOI. These advantages include:

- Massive scaling potential
- End to end addressing
- Improved network level security
- Auto-configuration
- Mobility
- Modular design with clean extensibility

Additional guidance on SOA and SOI can be found in the Practical Guide for Federal Service Oriented Architecture (PGFSA). The PGFSA can be downloaded at:

<http://smw.osera.gov/pgfsoa/index.php/Welcome>.

## 4.2 EA Driven IPv6 Planning

This section contains additional details describing how agencies can use EA to effectively plan for deploying IPv6-enabled network services.

### 1. Define Business Needs and Objectives.

The integration or implementation of any new technology must support an agency’s core mission areas, business needs, and strategic objectives.

IPv6-deployment can be:

- o Strategy-driven: Improving IT Infrastructure quality through security, reliability, agility;
- o Core mission-driven;
- o Bottoms-up operationally-driven: Involving technology refreshes or meeting OMB requirements.

**2. Define the Applications Supporting Each Function and the Services Provided by Each Application (Enabling Each Business Function). Identify Potential IPv6-Enabled Services.**

Once a strategic perspective for IPv6 integration is defined at the business level, the next step is to develop an understanding of the environment in which the new protocol will be integrated. For this effort, it is important to review the Service Component Reference Models for each IT investment that will be effected by a change in network protocols.

This step goes beyond developing or updating an inventory of network devices to evaluate their readiness to support IPv6 features. It is important to note that IPv6 is an update of existing TCP/IP technologies; therefore any device, service, or application that currently uses TCP/IP is in the scope of this assessment.

Listed below are examples of network services/IPv6 Capabilities that may be used to support your core mission applications. Please note that this is not an exhaustive list but should be used for guidance.

Each of the network services/IPv6 capabilities listed is mapped to a Functional Category specified in NIST Special Publication 500-267 - “A Profile for IPv6 in the U.S. Government – Version 1.0” (<http://www.antd.nist.gov/usgv6/usgv6-v1.pdf> ).

**Table 3 – Potential IPv6-Enabled Network Services**

| Functional Category     | Notes - Examples  |
|-------------------------|---|
| IPv6 Basic Capabilities | IPv6, ND, SLAAC, DHCP, FTP, DNS, E-mail, Printing, Network file system, Web Access (HTTP/HTTPS), Internet Information Services, Directory services  |
| Routing Protocols       | OSPF, BGP   |
| Quality of Service      | DiffServ  |
| Transition Mechanisms   | Dual Stack, Tunneling, 6PE  |
| Link Specific           | IP over X, ROHC   |
| Addressing              | IPv6 global, ULA, CGA   |
| IP Security             | IPsec, IKE, ESP, Cryptographic Algorithms   |
| Network Management      | SNMP, MIBs  |
| Multicast               | MLDv2, PIM-SM   |
| Mobility                | MIP, Nemo, Voice over Internet Protocol (VoIP) Transport Services, Internet Protocol Telephony (IPT) Services, Internet Protocol Facsimile (IP Fax) Services, Internet Protocol Video Transport, Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metro Area Network (WMAN), and Wireless Wide Area Network (WWAN) technologies, Instant Messaging Services, Unified Messaging Services, Radio over IP, Video Conferencing, TeleWork: <ul style="list-style-type: none"> <li>– Premise-based Virtual Private Network (VPN) services</li> <li>– Network-based VPN Services</li> <li>– Audio, video and data communications</li> <li>– Managed notebook/desktop support services</li> <li>– Security services</li> <li>– Application support through the Systems/Data Center services</li> </ul> |

| Functional Category                    | Notes - Examples  |
|--|---|
|  | – Customer support services through the Helpdesk and Desktop services |
| Application Requirements               | Sockets, DNS, URIs, guidance.   |
| Network Protection Device Requirements | Firewalls, intrusion detection systems, IPS                           |
| Miscellaneous                          | E-Learning, Video Surveillance, Video On-Demand, Asset Tracking       |

### 3. Identify Each Application's Technology Components, Assessing Changes Required

The technology architecture view should be updated

- Support the potential IPv6-enabled network
- Provide or require IP services and whether those assets, such as routers and servers, are capable of

This step also requires that the agency technology architecture be updated to address changes to:

- Additional technology infrastructure and standards necessitated by the need for IPv4/IPv6 interoperability, such as dual-stack
- Technology hardware and software products;
- The agency networking topology, if the agency technology architecture extends to

The Technical Reference Model (TRM) should be used as a basis for this effort, which should also

*The U.S. Postal Service (USPS) plans to deploy an IPv6-capable video surveillance system to 40,000 postal sites across the country. In addition to providing high-quality video, the system is expected to provide the USPS with enhanced mobility, security and network management capabilities. The new video platform will be integrated into the existing USPS network.*

*Because of the large number of USPS locations, their growing reliance on mobile devices and the increasing need for network-capable devices such as video cameras, postage meters and mail scanners, USPS expects IPv6 to be a gateway to enhancing its services and capabilities.*

*Dan Campbell,  
GCN Magazine. September 19, 20*

#### 4.2.1 Using the USG IPv6 Standards Profile

The US Government IPv6 Standards Profile was developed and released by the National Institute of Standards and Technology (NIST) to foster explicit IPv6 harmonization across industry/user groups. This IPv6 Profile is a strategic planning document to guide the acquisition of IPv6 technologies for operational Federal IT systems. Its intent is to:

- Define a minimal set of IPv6 recommendations to:
  - Deliver expected functionality
  - Insure interoperability
  - Enable secure operation
  - Protect early investments
- Define a compliance framework to:
  - Enable products to be tested against requirement sets
  - Document the results of such tests

Agency standards profiles or Technical Reference Models (TRMS) must align to the standards set forth by the USG IPv6 Standards Profile.

The Profile contains a detailed specification of IPv6 recommendations, allowing agencies to choose among the configuration options. The recommendations are organized:

1. Into subsets by “device” type (Host, Router, Network Protection Device)
2. By functionality (Base, Mobility, Routing, QoS, Transition, Link, Security, Multicast, Application, NPDs)
3. By requirement (Unconditional MUSTs, Conditional MUSTs, Optional Capabilities)

The USGv6 Profile is meant to provide a vehicle to communicate requirements and capabilities between USG design, specification and acquisition communities and networking vendors and system integrators. The USGv6 Test Program will provide an open, traceable means of verifying the correctness and interoperability of IPv6 capabilities claimed by individual products.

The USGv6-V1 Capability Check List in Annex-A of the USGv6 Profile, illustrated in Figure 4, provides a quick tabular means of conveying functional requirements and declarations of capabilities between the USG and its suppliers.

| Spec / Reference  | Section | USGv6-V1 Capability Check List<br>IPv6 Requirements      | Configuration Option | Device Type |          |     | Notes      |
|---|---------|--|----------------------|-------------|----------|-----|------------|
|   |         |  |                      | Host        | Router   | NPD |            |
| Note: Gray check boxes imply an atypical selection for device type. See profile text for details.             |         |  |                      |             |          |     |            |
| Note: <b>M</b> indicates category/context contains unconditional mandatory requirements. See NRT for details. |         |  |                      |             |          |     |            |
| SP500-267   | 6.1     | <b>IPv6 Basic Requirements</b>                           |                      | <b>M</b>    | <b>M</b> |     |            |
|   |         | support of stateless address auto-configuration          | SLAAC                |             |          |     | Host:[O:1] |
|   |         | support of SLAAC privacy extensions.                     | PrivAddr             |             |          |     | Host:[O:1] |
|   |         | support of stateful (DHCP) address auto-configuration    | DHCP-Client          |             |          |     |            |
|   |         | support of automated router prefix delegation            | DHCP-Prefix          |             |          |     |            |
|   |         | support of neighbor discovery security extensions        | SEND                 |             |          |     |            |
| SP500-267   | 6.6     | <b>Addressing Requirements</b>                           |                      | <b>M</b>    | <b>M</b> |     |            |
|   |         | support of cryptographically generated addresses         | CGA                  |             |          |     |            |
| SP500-267   | 6.7     | <b>IP Security Requirements</b>                          |                      | <b>M</b>    | <b>M</b> |     |            |
|   |         | support of the IP security architecture                  | IPsec-V3             | <b>M</b>    | <b>M</b> |     |            |
|   |         | support for automated key management                     | IKEv2                | <b>M</b>    | <b>M</b> |     |            |
|   |         | support for encapsulating security payloads in IP        | ESP                  | <b>M</b>    | <b>M</b> |     |            |
| SP500-267   | 6.11    | <b>Application Requirements</b>                          |                      |             |          |     |            |
|   |         | support of DNS client/resolver functions                 | DNS-Client           |             |          |     |            |
|   |         | support of Socket application program interfaces         | SOCK                 |             |          |     |            |
|   |         | support of IPv6 uniform resource identifiers             | URI                  |             |          |     |            |
|   |         | support of a DNS server application                      | DNS-Sever            |             |          |     |            |
|   |         | support of a DHCP server application                     | DHCP-Server          |             |          |     |            |
| SP500-267   | 6.2     | <b>Routing Protocol Requirements</b>                     |                      |             |          |     |            |
|   |         | support of the intra-domain (interior) routing protocols | IGW                  |             |          |     |            |
|   |         | support for inter-domain (exterior) routing protocols    | EGW                  |             |          |     |            |
| SP500-267   | 6.4     | <b>Transition Mechanism Requirements</b>                 |                      |             |          |     |            |
|   |         | support of interoperation with IPv4-only systems         | IPv4                 |             |          |     |            |
|   |         | support of tunneling IPv6 over IPv4 MPLS services        | 6PE                  |             |          |     |            |
| SP500-267   | 6.8     | <b>Network Management Requirements</b>                   |                      |             | <b>M</b> |     |            |
|   |         | support of network management services                   | SNMP                 |             | <b>M</b> |     |            |
| SP500-267   | 6.9     | <b>Multicast Requirements</b>                            |                      | <b>M</b>    | <b>M</b> |     |            |
|   |         | full support of multicast communications                 | SSM                  |             |          |     |            |
| SP500-267   | 6.10    | <b>Mobility Requirements</b>                             |                      |             |          |     |            |
|   |         | support of mobile IP capability.                         | MIP                  |             |          |     |            |
|   |         | support of mobile network capabilities                   | NEMO                 |             |          |     |            |

| Spec / Reference | Section | USGv6-V1 Capability Check List<br>IPv6 Requirements | Configuration Option | Device Type |        |     | Notes     |
|------------------|---------|---|----------------------|-------------|--------|-----|-----------|
|                  |         |   |                      | Host        | Router | NPD |           |
| SP500-267        | 6.3     | <b>Quality of Service Requirements</b>              |                      |             | M      |     |           |
|                  |         | support of Differentiated Services capabilities     | DS                   |             | M      |     |           |
| SP500-267        | 6.12    | <b>Network Protection Device Requirements</b>       |                      |             |        | M   |           |
|                  |         | support of basic firewall capabilities              | FW                   |             |        |     | NPD:[O:1] |
|                  |         | support of application firewall capabilities        | APFW                 |             |        |     | NPD:[O:1] |
|                  |         | support of intrusion detection capabilities         | IDS                  |             |        |     | NPD:[O:1] |
|                  |         | support of intrusion protection capabilities        | IPS                  |             |        |     | NPD:[O:1] |
| SP500-267        | 6.5     | <b>Link Specific Technologies</b>                   |                      | M           | M      |     |           |
|                  |         | support of robust packet compression services       | ROHC                 |             |        |     |           |
|                  |         | support of link technology                          | Link=                | M           | M      |     | [O:1]     |
|                  |         | (repeat as needed) support of link technology       | Link=                |             |        |     |           |

Figure 4 – USGv6-V1 Capability Check List – Annex A

USGv6 Node Requirements table further expands each of the configuration options above into a detailed list of IETF standards and additional requirements necessary to conform to the USG user requirements expressed through the check list.

| RFC              |         | Functions  |        |      | Requirements by device |       |        |     | Effective |
|------------------|---------|--|--------|------|------------------------|-------|--------|-----|-----------|
| Spec / Reference | Section | USGv6-V1 Node Requirements<br>Title / Definition | Status | Year | Condition / Context    | Host  | Router | NPD | Date      |
|                  |         | <b>Multicast Requirements</b>                    |        |      |                        |       |        |     |           |
| RFC3810          |         | MLD Version 2 for IPv6                           | PS     | 2004 |                        | M     | M      |     | 2010/03   |
| RFC4607          |         | Source-Specific Multicast for IP                 | PS     | 2006 | SSM                    | c(M)  | c(M)   |     | 2010/03   |
| RFC4604          |         | MLDv2 for Source Specific Multicast (SSM)        | PS     | 2006 | SSM                    | c(M)  | c(M)   |     | 2010/03   |
|                  |         | <b>Protocol Independent Multicast (PIM)</b>      |        |      |                        |       |        |     |           |
| RFC4601          |         | PIM Sparse Mode (SM)                             | PS     | 2006 | SSM                    |       | c(S+)  |     |           |
| RFC4609          |         | PIM-SM Security Issues / Enhancements            | INF    | 2008 | SSS                    |       | c(S)   |     |           |
| RFC3956          |         | Embedding Rendezvous Point (RP) Mcast Addr       | PS     | 2004 | SSM                    |       | c(S+)  |     |           |
|                  |         | <b>Mobility Requirements</b>                     |        |      |                        |       |        |     |           |
| RFC3775          |         | Mobility Support in IPv6                         | PS     | 2004 | MIP                    | c(M)  | c(M)   |     | 2010/03   |
|                  | 8.1     | All Nodes as Correspondent Node                  |        |      | MIP                    | M     |        |     | 2010/03   |
|                  | 8.2     | Route Optimization                               |        |      | MIP                    | c(M)  |        |     | 2010/03   |
|                  | 8.2     | Allow route optimization to be disabled          |        |      | MIP                    | c(M)  |        |     | 2010/03   |
|                  | 8.3     | All IPv6 Routers                                 |        |      | MIP                    |       | M      |     | 2010/03   |
|                  | 8.4     | Home Agents                                      |        |      | MIP                    |       | c(M)   |     | 2010/03   |
|                  | 8.5     | Mobile Nodes                                     |        |      | MIP                    | c(M)  |        |     | 2010/03   |
| RFC4202          |         | The Network Access Identifier                    | PS     | 2005 | MIP                    | c(S+) | c(S+)  |     |           |
| RFC4283          |         | Mobile Node Identifier option for MIPv6          | PS     | 2005 | MIP                    | c(S+) | c(S+)  |     |           |
| RFC4877          |         | MIPv6 Operation with IKEv2 and IPsec-v3          | PS     | 2004 | MIP                    | c(M)  | c(M)   |     | 2010/03   |
| RFC3963          |         | Network Mobility (NEMO) Basic Support            | PS     | 2005 | NEMO                   |       | c(M)   |     | 2010/03   |

Figure 5 – Sample USG IPv6 Profile Excerpt

### 4.3 Developing an IPv6 Transition Strategy Plan

The IPv6 Transition Strategy Plan should be folded into the Enterprise Transition Strategy Plan, should link to core mission segments as appropriate, and should define a specific timeline and set of milestones to deploy the IPv6-enabled network services defined in the IT Infrastructure Segment Architecture.

As with any other technology integration effort, the planning effort should consider multiple timelines, including:

- Budget cycles
- Technology refresh cycles
- IT Infrastructure quality improvements
- Equipment and software certification cycles
- IT project dependencies
- Technology standards development and adoption
- Software development life cycle

When developing the transition strategy, focus on ensuring that network, computing, application, and service components are enabled in a sequence that will generate maximum benefit to the business mission through meaningful end-to-end IPv6 activity. At times, an immediate incremental change has advantages over waiting for all IPv6 features to be available in the next version of a product.

Elements that your Transition Strategy must include are:

1. Identification of transition priorities
2. Identification of transition activities
3. Transition milestones
4. Transition criteria for legacy, upgraded, and new capabilities
5. Dependencies
6. Risks and mitigation strategies
7. Maintenance of interoperability and security during transition
8. Use of the USGv6 Profile to express IPv6 capability requirements for specific products
9. Transition governance:
  - Policy
  - Roles and responsibilities
  - Management structure
  - Performance measurement
  - Reporting
  - Management actions
10. Training
11. Testing

Please refer to RFC 5211 “[An Internet Transition Plan](#)” for additional guidance.

## 4.4 Integration with Capital Planning

Agencies should develop and submit Exhibit 300 business cases to invest in the IPv6 vision defined by their IT Infrastructure Segment Architecture and Transition Strategy Plan. This approach corresponds directly to the FEA PMO’s Performance Improvement Lifecycle shown below.

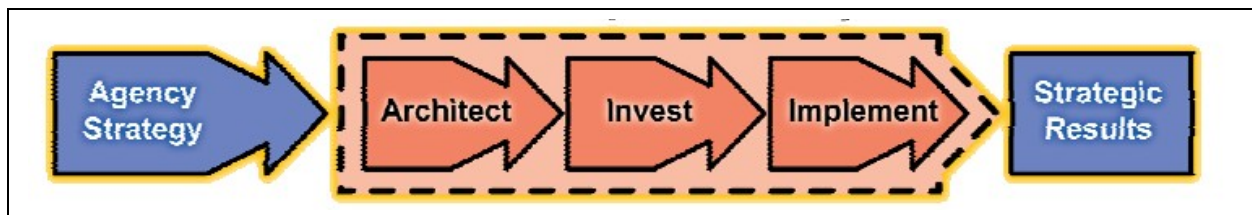


Figure 6 – FEA PMO’s Performance Improvement Lifecycle

The Exhibit 300 should include:

- A business justification that addresses the value of the IPv6-enabled network service and performance/quality gaps which will be addressed;

- Appropriate SRM and TRM mappings, as defined in the IT Infrastructure Segment Architecture. Technologies should be compliant with agency guidelines and the USG IPv6 Profile released by NIST; and
- Performance commitments and delivery milestones that match those defined in the Enterprise Transition Strategy Plan.

Agencies should require all future technology refresh spending to incorporate IPv6. Other OMB IT initiatives, such as common security configurations, reduced external Internet connections and coordinated infrastructure spending, should all be considered in conjunction with the move toward IPv6-enabled networks and devices

Agencies should begin to submit business cases for IPv6-enabled Network Services during the FY2011 Select Phase.

It is expected that proactive, architecture-based planning, procurement controls, and leveraging Blanket Purchase Agreements (BPAs) will result in cost savings and avoidance. Current federal IT spending, including IT infrastructure, can be viewed through OMB's Visualization to Expenditures in Information Technology (VUE-IT) tool, found at <http://www.whitehouse.gov/omb/egov/vue-it/index.html#path5/path5.json|path2/path2.json>.

## **4.5 OMB IPv6 EA Assessment Criteria**

The Federal Enterprise Architecture Program Management Office will assess each agency's IPv6 transition progress through the Enterprise Architecture Assessment Framework (EAAF). OMB requires that "the agency's EA (including enterprise transition plan and segment architecture) must incorporate Internet protocol version 6 (IPv6) into the agency's IT infrastructure segment architecture and IT investment portfolio. The agency must have concrete plans to deploy IPv6-enabled mission services and applications in its environment."<sup>8</sup>

According to the OMB EAAF Version 3.0 (<http://www.whitehouse.gov/omb/e-gov/fea/>), agencies will be required to meet the following IPv6-related criteria depicted in the following table.

It is important to note that each "level" is intended to build upon previous levels (for example, an agency cannot achieve a Level 4 without successfully demonstrating completion of Levels 1, 2, 3, and 4).

**Table 4 – IPv6 Criteria in the Enterprise Architecture Assessment Framework v3.0**

|                                 |  |
|---------------------------------|--|
| <p><b>Level 1 Practices</b></p> | <p><i>Activities:</i> The agency has performed a cost and risk impact analysis for migrating to IPv6. Agency has also completed a second inventory of IP-aware devices.</p> <p><i>Artifacts:</i> IPv6 impact analysis document using guidance in Attachment B of OMB M-05-22; second IP-aware device inventory (Attachment A)</p>  |
| <p><b>Level 2 Practices</b></p> | <p><i>Activities:</i> The agency has met all of its IPv6 transition milestones, and is on schedule to complete transition per OMB M-05-22.</p> <p><i>Artifacts:</i> IPv6 transition milestones (included in the enterprise transition plan) through completion date showing projected and actual completion dates, evidence of milestone completion (agency should determine the artifact(s) constituting evidence of completion for each milestone), documentation of successful execution of deployment test criteria (once transition is complete).</p> |
| <p><b>Level 3 Practices</b></p> | <p><i>Activities:</i> The agency has incorporated IPv6 modernization activities into its IT infrastructure segment architecture.</p> <p><i>Artifacts:</i> IT infrastructure segment architecture</p>   |
| <p><b>Level 4 Practices</b></p> | <p><i>Activities:</i> The agency has made concrete plans (e.g., stood up an IT investment with an Exhibit 300 business case, etc.) to deploy IPv6 enabled network services in its environment.</p> <p><i>Artifacts:</i> IT infrastructure segment architecture, Exhibit 53, Exhibit 300s</p>   |
| <p><b>Level 5 Practices</b></p> | <p><i>Activities:</i> The agency has made concrete plans (e.g., stood up an IT investment with an Exhibit 300 business case, etc.) to deploy IPv6 enabled mission services and applications in its environment.</p> <p><i>Artifacts:</i> IT infrastructure segment architecture, Exhibit 53, Exhibit 300s</p>  |

## Section 5:

## Transition

*"IPv6 is like an urban redevelopment and expansion. It is all about understanding the need of the stakeholders and enabling it for future growth. The US Government is showing leadership in planning ahead, preparing for this major (and much needed) technology shift and its innovative enhancements for the 21st century always on communication era."*

**Yanick Pouffary,  
IPv6 Forum Fellow,  
North American IPv6 Task Force  
Technology Director**

## Milestones

After agencies develop their IT Infrastructure Segment Architectures (incorporating IPv6 modernization plans) they should develop an IPv6 Transition Strategy to describe how their defined future vision will be attained (please see Section 3.3 for additional guidance on how to develop an IPv6 Transition Strategy).

IPv6 deployment must be carried out within an agency's IT governance framework in order to minimize data and application risks.

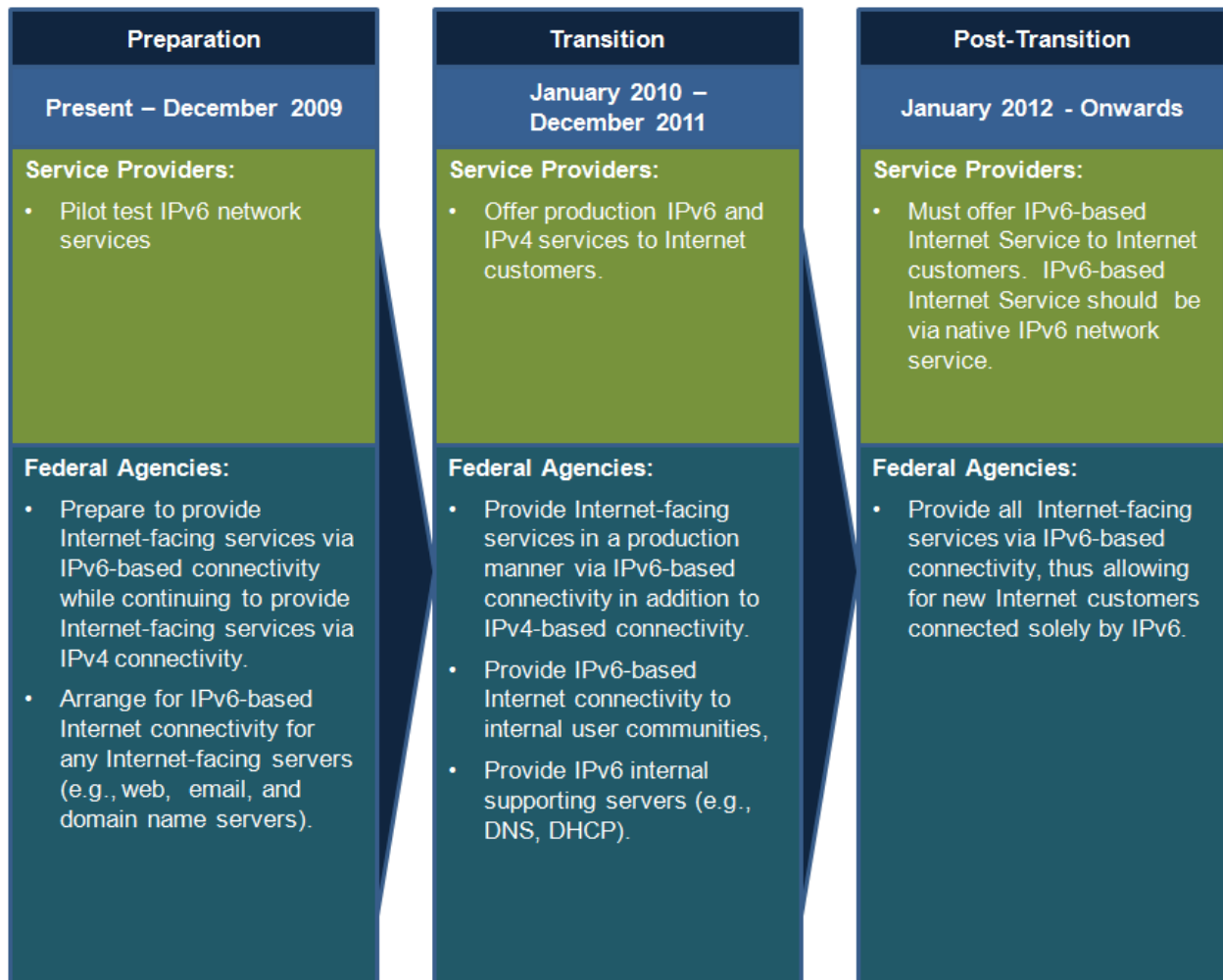
This section provides a comprehensive overview of common IPv6 Milestones that should be incorporated into IPv6 Transition Strategy Plans, as well as "quick wins" that agencies should address even before planning for IPv6-enabled network service deployment.

Organizations do not have to transition to IPv6 all at once. Rather, by integrating IPv6 in phases, IT staff members can learn what they need to know to help their agencies begin experiencing the benefits of IPv6 while the integration is underway.

According to Request for Comment (RFC) 5211 (dated July 2008), which can be found at <http://www.ietf.org/rfc/rfc5211.txt>, there are three phases for transitioning the Internet from a predominantly IPv4-based connectivity model to a predominantly IPv6-based connectivity model<sup>9</sup>. These phases are:

1. Preparation
2. Transition
3. Post-Transition

A proposed timeline for these phases has been developed so that the Post-Transition Phase will occur prior to IPv4 address pool exhaustion. The following graphic provides a high-level summary of each phase, the associated timeframe, and key activities that service providers and federal agencies should strive to address.

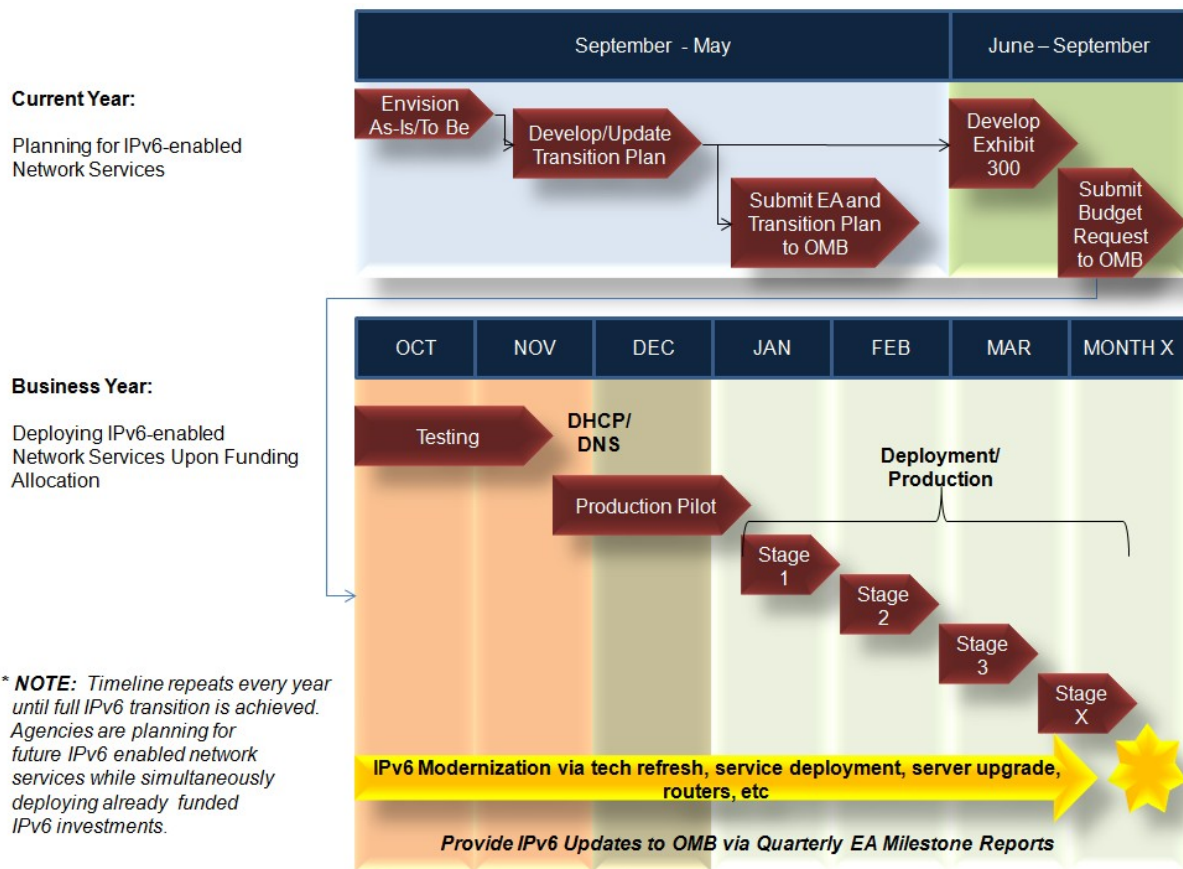


**Figure 7 – IPv6 Transition Phases and Timeline**

A further breakdown of this high-level timeline is illustrated on the following page, depicting Enterprise Architecture and Transition Strategy Plan development and the Capital Planning and

Investment Control process. This timeline assumes a full-year of planning for the deployment of IPv6-enabled network services and approximately 3 ½ months of testing and piloting.

Note: NON-public facing networks on private subnets or point-to-point leased lines that do not rely on carrier transport across the Internet core do not have a driver to migrate to IPv6 by 2012 and SHOULD migrate through gradual tech refresh.



**Figure 8 – Proposed Timeline for IPv6 Transition**

By taking a phased approach to IPv6 integration, the IT staff can selectively choose where to use IPv6 as the project progresses. Other advantages of the phased approach are:

- The IT group can gradually gain skills and confidence.

- The IT group can develop best practices during the early phases, which helps to expedite the IPv6 integration across the enterprise.
- Agency managers and IT groups can confirm that IPv6 provides business value and is stable, manageable, and secure enough to be deployed.

During each phase, one should approach IPv6 integration from a systems perspective, considering people, processes and controls, and technology.

## 5.1 Quick Wins

In concert with developing initial IPv6 modernization plans through the IT Infrastructure Segment Architecture and IPv6 Transition Strategy Plan, it is recommended that agencies undertake the following activities to accelerate their preparation for IPv6-enabled network service deployment.

### 5.1.1 Establish an IPv6 Test Lab

The total testing strategy discussed in this document includes general purpose IPv6 device testing that is appropriate for all Agencies, covered in Section 1.3.2 “IPv6 Test Program”. Agency specific deployment and acceptance testing guidance is provided in this section.

Setting up a test lab is important for the safe controlled introduction of new technology into your network and prototyping with an emphasis on small scale validation of targeted performance outcomes (e.g. experimenting with secure IPv6-enabled teleworking). Testing in a lab enables the agency IT group to perform tests that could potentially be disruptive or introduce a security risk if deployed on the production network. The test environment should be set up as close as possible to resemble the production environment. At first, the test sites should not be connected to the production network or to each other. Later, after successful intra-site testing, connect them to each other to test inter-site routing and connectivity. During the testing phase, the IT team will gain valuable experience with integrating IPv6 into the network which will allow them to determine if the technology plan or schedule needs to be modified.

It is important to determine if an agency will be required to perform IPv4/IPv6 protocol translation to allow pockets of IPv6 hosts to communicate with legacy IPv4 hosts. If this is the case, the lab should provide connectivity for all clients and servers between IPv4 and IPv6, regardless of network placement. Test cases should include IPv6 to IPv4, IPv4 to IPv6, and IPv6 to IPv6 communication. The test lab should contain a central router providing routing between IPv4-only, IPv6-only, and IPv4/IPv6-mixed LANs as well as protocol translation gateways. A variety of IPv4-IPv6 protocol translation technologies are being defined presently within the IETF. A key activity of the test lab should be verification of non-impact to IPv4-only applications when traversing intervening IPv6 networks.

During intra- and inter-site testing, document successful configurations as well as interoperability issues. Test planned IPv4-IPv6 dual-stack, tunneling and translation

**Tip:** Many unexpected results during IPv6 testing are due to the mis-configuration of LAN and VLAN segments of services required to support IPv6, such as DNS. This underscores the importance of training and hands-on experience before IPv6 is deployed in an operational environment.

technologies. Induce failure conditions such as router unavailability, DNS server mis-configurations, link outage, etc. to identify and document observed behavior of networking and application elements. Explore alternative workarounds to each simulated outage and observe suitability of resolution. This information will be helpful after rolling into production to aid in troubleshooting and to expand the experience and comfort level of IT staff members.

After IT staff members in each lab develop solid competence with IPv6, begin production LAN deployment in a few locations. During this phase, the pilot site infrastructure should be “IPv6-enabled”. Set up routers and switches to process IPv6 traffic and configure the LAN to transport the agency’s IPv6 prefixes to production host computers, printers, and other devices. Ensure that the security architecture is configured to handle both IPv4 and IPv6 and set up the DNS and DHCP servers to handle IPv6 queries. Implement the selected IPv4-IPv6 co-existence technologies; this may be a translation gateway interconnecting this new IPv6-only subnet to IPv4/IPv6 networks, tunneling or dual-stack implementations. Configure the associated Network Management Systems (NMSs) to monitor the IPv6 network and infrastructure and as part of the pilot, set up one or more applications that can run over IPv6 so that the agency can begin building experience of IPv6 within their environment.

### 5.1.2 External Facing Servers

External facing eCommerce servers, mail gateways, instant messaging servers, Web servers, and voice over IP gateways hosting portals for remote clients, teleworkers, partner agencies, and group collaboration all have to serve content across the Internet backbone to external hosts. ***Because of IPv4 address depletion and its effect on core routing, applications that rely on the Internet core for transport to external hosts should upgrade first to IPv6-capable versions by 2010.***

Next, upgrade host interfaces such as Web servers and e-mail clients that will have to connect to external servers.

Lastly, upgrade internal facing systems in an Enterprise LAN as a third priority, as these systems can continue to rely on IPv4 NAT addresses for some time.

Since sites will transition to IPv6 in a phased approach, the best plan forward for web servers is to simply enable dual-stack addressing with both IPv4 and IPv6 addresses and ensure that there is either a native or tunneled IPv6 path between all IPv6 clients and the servers. Web servers should have both their IPv4 and IPv6 addresses configured into DNS servers.

#### **Tips:**

For Internet (external) reachable hosts, such as gateways and web, email and DNS servers, configure IPv6 addresses according to the address and security plans. These devices will likely require both IPv4 and IPv6 addresses to enable reachability from IPv4 and IPv6 web browsers, email servers, etc. Validate firewall settings to enable defined IPv6 traversal addresses according to the address and Internet security plans. Verify proper IPv4/IPv6 address resolution in DNS.

## 5.2 IPv6 Network Service Deployment

### 5.2.1 Develop Addressing and Routing Plan

An escalating demand for IP addresses acted as the driving force behind the development of the larger address space offered by the IPv6. According to industry estimates, in the wireless domain, more than a billion mobile phones, Personal Digital Assistants (PDA), and other wireless devices will require Internet access; each needing its own unique IP address.

The extended address length offered by IPv6 eliminates the need to use techniques such as network address translation to share scarce globally unique addresses.

Addressing Plans should:

- First and foremost concentrate on hierarchical routing information by distributing address blocks for major enterprise network locations before breaking network blocks into separate subnets for varying security and QOS support levels. The addressing structure must follow the network topology.
- Account for evolving government requirements such as Trusted Internet Connection (TIC), Networkx, security, Continuity of Operations (COOP), and geographical diversity.
- Be stored in a secure and auditable database for IPv4 and IPv6 networks, blocks, and subnets. This “plan of record” database serves as the basis for address status, moves, adds, and changes. Reports and audit information are useful in managing and troubleshooting.

### 5.2.2 Address Acquisition

Acquiring IPv6 address space is certainly a key step in planning a transition to IPv6. IPv6 space can be obtained from the American Registry of Internet Numbers (ARIN) for North American based networks. Other Internet Registries exist for address assignment in other parts of the world: RIPE for Europe, APNIC for Asia/Pacific, LACNIC for Latin America/Caribbean, and AfriNIC for Africa.

The ARIN website, [www.arin.net](http://www.arin.net) contains application templates and fee schedules for IPv4 and IPv6 allocations. The current process for obtaining IPv6 address space entails completing an IPv6 network request template, which requires information about points of contact, IPv6 allocation plans, and DNS reverse mapping name server hostnames, among other items. Once the template is submitted to ARIN, the template is reviewed and ARIN will respond within three business days requesting further information or providing approval. Once approved, payment of the annual fee is required along with execution of a Registration Services Agreement. Once these tasks are completed, the address space will be allocated.

The amount, or size of space allocated depends on the address space requirements and role of the applying entity in requesting the allocation. Thus, if the requesting entity is an end user, a smaller block will be allocated; if the requesting entity performs the role of a Local Internet Registry (LIR) which allocates space further to other organizations, ARIN will allocate a larger block.

The IPv6 addressing architecture defines unique local address (ULA) space as address space that may be used internally and is not routable on the public Internet. This address space is analogous to RFC1918 private address space in IPv4. While not Internet-routable, ULA network uniqueness is nonetheless desired to minimize the probability of overlapping ULA space among private inter-organizational interconnections. To increase the probability of uniqueness of this local address space, the global ID portion of the address prefix must be pseudo-randomly generated as recommended by RFC 4193. The end result is an entirely locally administered /48 prefix for use within the organization while also enabling global IPv6 Internet reachability without requiring NATs.

Agencies should develop policies and criteria to define which agencies or organizations may obtain address space from other organizations or directly from ARIN or ISPs. Policies regarding the use of ULA space should also be developed. These policies should be reflected in addressing management approaches, and should be incorporated in addressing plans.

### **5.2.3 Establish Address Management and Allocation Procedures**

Address management is crucial to assuring unique and consistent IPv6 subnet and address assignments, not to mention accurate configuration of associated DNS and DHCPv6 services. To assure this uniqueness and consistency, an IPv6 address management tool should be deployed. Such a tool must have the capability to track, allocate, and manage IPv6 space as well as that of IPv4.

Given that IPv6 will be deployed “over” existing IPv4 networks in dual-stack deployments or in tunneling and translation environments, it is important to understand the potential impacts of segregated IPv4 and IPv6 address management approaches. Combined IPv4/IPv6 address management schemas are available and should be considered. IPv6 address assignments to servers will require host name lookups via DNS (unless users can reliably type in IPv6 addresses in their browsers). The use of DHCPv6 should be assessed to determine whether it will be used for one or more of the following: address assignment, parameter assignment only, or prefix assignment; configuration of DHCPv6 accordingly should be provided by the address management tool.

Address management should also include various IPv6 address allocation mechanisms, including manual, best-fit, random and sparse. The sparse algorithm is useful at the top layer of the allocation hierarchy to “spread out” top level allocations to accommodate future growth. Best fit allocations preserve address space by using contiguous blocks where possible and may be effective in the middle of the allocation hierarchy. At the bottom, the subnet level, random allocation may be desired to obfuscate subnet number (instead of counting up from 1) for privacy purposes. These procedures should be adapted as appropriate and documented within the organization.

The address management database is only as accurate as the information that goes into it. Some form of address discovery and reconciliation should be considered to enable comparison of the database with actual network information. Such discovery for IPv6 subnets will likely require Neighbor Discovery Cache table reads since a brute force ping sweep of host IDs is unfeasible (one of the down sides of such a large address space is that scans are just as difficult for legitimate purposes as malicious ones). However accomplished, the discovered information should be stored as snapshots for historical comparison and reclaim. Auditing of IP address

occupancy is important for troubleshooting and accountability tracking, and a reclaim function can be used to free up addresses or subnets that are no longer in use given a sample set of discovery information. Address auditing is important to prevent the proliferation of unused address blocks and the resulting discontinuous production address space and reduction of routing aggregation that will result. Additionally, regional address registries will require address auditing and accountability of future IPv6 address acquisition is necessary, as all acquisitions are based on operational need.

A list of specific Address Management and Allocation Procedures includes:

- Access existing IP address management and allocation governance and procedures.
- Develop and promulgate new/revised IPv6 address management and allocation governance including requirements, guidance, policy, procedures, and reporting.
- Determine IP address allocation and recovery lifecycle process.
- Identify and acquire an automated IP Address management (IPAM) and allocation tool or appliance. The use of an address management tool is not a requirement, but given the nature and size of IPv6 address blocks, wide-areas and local networks can easily grow to a level of complexity that will be unmanageable. Additionally, address registries may require an address auditing function, which can become exceedingly complex if accomplished on spreadsheets. For growth and auditing purposes, it is highly recommended that an address management tool be considered. Tool/Appliance capabilities should include the following:
  - Dynamic address request/allocation and recovery
  - Pre-allocate and reserve address blocks
  - Discovery and identification of utilized, unutilized, and overlapping address space ranges
  - Address plan templates and development tools
  - Delineate address blocks by network, organization, geographic location, function, etc.
  - Network Device configuration support and file management
  - Import network definitions from network devices
  - Variable access right to multiple administrators
  - Articulate and define address space authority boundaries
  - Join or split networks
  - Comprehensive searches
  - Audit features and logs which provide statistical analysis
  - Storage and feedback on Registrar requirements, information, and correspondence
  - DNS administration support and zone transfer/management
  - Predefined and definable event “triggers”

#### **5.2.4 Domain Name Service (DNS) Assessment**

This task involves the assessment and transition planning of the organizations Domain Name Service. It should be noted that networking functionality and interoperability, in an IP environment, is not possible without an operational DNS. The Top-Level Domain .GOV and all lower level Department and Agency domains must be capable of managing and responding to IPv6 address queries for IPv6 networking to occur.

Specific actions include:

- Requirements: Develop DNS transition requirements for the organizations infrastructure based on the address and routing plan and organizational domains, locations, functions, etc. Determine the span of DNS domains. Note that DNS address spaces are independent of address spaces/network topology. RFC4472 (<http://www.ietf.org/rfc/rfc4472.txt>) discusses name space fragmentations, and operational considerations and issues associated with IPv6 DNS.
- Inventory: Conduct an inventory of existing DNS infrastructure and servers, including the current versions of DNS software, such as BIND.
- Upgrades guidance: Develop comprehensive guidance for the upgrade of DNS servers and software. This guidance should include procedures and best practices.
- Separation: The initial transition to IPv6 capability for DNS should incorporate a philosophy of separation rather than integrated dual-stack functionality, i.e., leave the existing IPv4-only DNS servers alone and functioning normally and implement new dual-stack DNS servers, in required pairs, separated by security procedures. Once the IPv6 capable DNS is active and the organization has confidence in the new system, then the servers can be integrated. The physical and/or logical separation of IPv4 and IPv6 capabilities and services will provide additional security in all facets of the network and application environment.
- DNS demonstration: DNS should be demonstrated in a laboratory setting first, then as a companion service to IPv4-only DNS, and subsequently as a separate production service.
- Future Upgrades: Plan for future upgrades to the IPv6 capable DNS and continue to plan for and incorporate system upgrades.
  - Implementation of unicast vs. anycast addressing for DNS: Unicast DNS is the current mode of operation for the IPv6 DNS infrastructure. IPv6 will permit the use of anycast addressing, providing potential increases in reliability and flexibility of DNS.
  - DNSSEC: Investigate and implement DNSSEC security features in operational IPv6 DNS servers. DNS security extensions, DNSSEC, defined in RFCs 4033-4035, provide a means to authenticate the origin of resolution data within DNS and to verify the integrity of that data. Thus, DNSSEC provides a means to detect packet interception, ID guessing, and cache poisoning attacks. In fact, DNSSEC was acknowledged as the only comprehensive solution to the recent Kaminsky cache poisoning bug. The operation of DNSSEC relies on digital signatures to enable data origin authentication and end-to-end data integrity verification. ISC's BIND DNS server implementation supports DNSSEC and provides two core utilities required to generate private/public key pairs and to sign zones using these keys. Signing zones deployed on DNS servers enable resolvers and servers obtaining authoritative information from such DNS servers to authenticate the origin or resolution data and to verify the integrity of that data.

In summary, DNSSEC administration requires processes and procedures for key generation, zone signing, key distribution, and key rollovers. IT staff must be well versed in DNSSEC technology to monitor and troubleshoot secure resolution issues.

## 5.2.5 DHCPv6 Assessment

DHCPv6 performs a variety of functions. It can be used to assign IPv6 addresses and option parameters as does DHCP for IPv4 or it can be used simply to supply IP parameter options to clients that have auto-configured addresses. The assessment required entails consideration of the trade-offs of implementing DHCPv6 vs. use of stateless address auto-configuration (SLAAC).

In a stateful address assignment model, the DHCPv6 server provides the IPv6 address and associated device IP parameters (e.g. address of a recursive DNS server, etc). This mimics the DHCP for IPv4 approach and gives the network administrator the most control by defining who can get an address (e.g., using MAC address filtering to identify acceptable clients), what address is assigned, and what additional parameter values are assigned. While providing the most control, it does require proper configuration and administration, though an IP address management system can help ease this burden by associating address pools in the address plan with configuring corresponding DHCPv6 server address pools.

Stateless address auto-configuration (SLAAC) entails a client identifying the IPv6 subnetwork prefix through router advertisements, calculating of its own interface identifier, and concatenating these fields to derive a global IPv6 address. After verifying uniqueness through the duplicate address detection process, the derived IPv6 address may be used. However, this stateless auto-configuration may not sufficiently configure the device to communicate on the IPv6 network. For example, what DNS servers are available on or near this subnet to resolve hostnames to IPv6 addresses? This and other information may be obtained via DHCPv6. Use of SLAAC for address assignment and DHCPv6 for parameter assignment is sometimes referred to as stateful/stateless hybrid approach.

Prefix delegation entails the assignment of an entire prefix or subnet address. This function is useful in environments where devices downstream in the routing topology request a prefix for use; which automates subnet assignment and encourages IPv6 addressing hierarchy. While the DHCPv6 protocol is used for this function, the actual disseminator of subnets may be a router. A policy should be defined regarding prefix delegation. The fundamental question becomes, should devices be enabled to request subnets or should this function reside under the control of the IP address planning team?

Use of dynamic DNS is optional but very useful in automatically updating DNS with hostname and IP address information, particularly for DHCP clients. The DHCP server can be configured to update DNS based on leases dispensed to clients. The server can also allow the client to perform the update itself, though this is typically frowned upon in enterprise environments due to security concerns. However, if SLAAC is used, and auto-configured hostnames and IP address assignments appear in DNS, then either the client must be permitted to update DNS using DDNS or the centralized IP inventory administrator must perform such an update manually.

If the DHCP server updates DNS, the ISC DHCP server can be configured to sign the update using transaction signatures (TSIG). The BIND DNS server receiving the update can likewise be configured to authenticate the TSIG and also to constrain what source IP addresses or subnets from which DDNS updates may be accepted. For non-dynamic clients, e.g., servers and routers, addresses are entered manually and should be tracked using a centralized IP database. Such updates may also trigger DDNS updates from the IP database to the corresponding master DNS server.

As discussed above, IP parameters other than IPv6 addresses can also be assigned by DHCPv6 servers. These parameters, in the form of DHCP options, can be configured with values for assignment to clients. Different client devices may require different or unique parameter values, e.g., VoIP devices vs. plain old data devices. The DHCPv6 server can be configured to recognize these different device types by analyzing the vendor class identifier, user class identifier, MAC address, or other parameter within the DHCPv6 packet. Once matched on a value, the DHCPv6 server may then assign the corresponding options. For example, a VoIP phone may supply a value of “VOIP” within its vendor class identifier option and if the DHCPv6 server is configured to recognize clients providing this value in the vendor class identifier field, it can provide the corresponding VOIP options.

### 5.2.6 Network Management

IPv4-based network management and fault tracing tools must undergo significant change to properly manage IPv6 networks.

Network Management considerations include:

- No dependencies on IPv4 transport or services
- Ability to utilize IPv6 neighbor discovery to perform network mapping features
- Upgraded for the latest dual-stacked Management Information Bases (MIBs)
- Database and/or storage structures upgraded for IPv6
- GUI and documentation upgraded for IPv6

The resulting capabilities are:

- Full GUI interface for IPv6 features
- Ability to discover and manage IPv6 devices
- Ability to map IPv6 networks
- Ability to detect status of IPv6 services such as DHCPv6, IPv6 Routers, IPv6-capable DNS services

### DREN Success Story

The Department of Defense's (DoD's) High Performance Computing Modernization Program (HPCMP) is responsible for providing some of the world's most advanced computing capability in support of the DoD mission. The nation-wide Defense Research and Engineering Network (DREN) provides the HPCMP user community with protocol-rich, high-availability, high-capacity, low-latency, secure connectivity. In June, 2003, the DREN was designated as the first DoD IPv6 pilot network.

The goals of the DREN IPv6 pilot were to:

End-to-end IPv6-enable the DREN wide-area network (WAN).

Maintain pre-pilot performance and security levels.

IPv6-enable the infrastructure at selected sites.

IPv6-enable a core mission application.

Document and share lessons learned.

By July 2005 the entire DREN WAN was routinely supporting end-to-end IPv6 traffic. Several sites were supporting IPv6 along with IPv4. A core mission application providing authentication and end-to-end access was IPv6-enabled. Performance and security levels were as good as and in some ways better than before.

Six keys to success and eight challenges overcome in accomplishing this without additional personnel and with less than \$100,000 in additional funding are described in the DREN Success Story, available on the E-Gov Success Stories and Case Studies Website: <http://www.whitehouse.gov/omb/e-gov/fea/>.

Tracking IPv4 and IPv6 address space in a centralized inventory database is recommended. This includes subnets as well as individual address assignments. Implementing inventory assurance functionality can help ensure the accuracy of the IPv4/IPv6 address space. Gathering actual address assignments and reconciling against the centralized inventory provides this assurance.

Using SNMP to read router interface and IP address tables provides one example mechanism to discover subnet allocations at the router interface level. This discovered subnet information can be compared with the corresponding IP address inventory to identify misprovisioned, or "rogue", subnet assignments.

Discovery at the IP address level is typically performed on IPv4 networks using one or more available mechanisms such as ping, ARP cache discovery, DNS lookups, or additional port open packets. Many of these techniques are not practical for IPv6 subnets. Passive subnet snooping, neighbor discovery, and gathering IPv6 addresses from subnet routers are possible IPv6 host discovery mechanisms. While gathering IP occupancy is important, the post-processing of discovered host information by comparing actual address assignments with the corresponding IP address inventory is equally important in providing an exception report highlighting discrepancies. Such a report saves time otherwise required to manually compare discovery output with the IP database.

### 5.2.7 Application Development

This effort addresses the planning for and development or modification of existing IP applications to be IPv6 capable.

Specific application development actions include:

- **Planning for Application Transition:** All networked applications, including clients and servers need to be modified or redesigned to function in an IPv6 networking environment. Initially, applications will be required to perform common IPv6 functions and will need to evolve to incorporate more advanced features of the protocol. The planning for IPv6 application transition should include:
  - Application Inventory
    - Agency Government-off-the-shelf (GOTS) applications
    - Commercial-off-the-shelf (COTS) applications
    - Existing Application upgrades and refresh
    - New application developments and procurements
    - Applications at end-of-life
  - Assessment of legacy operating systems and applications to determine whether to include in the transition, use a transition mechanism, or retire the application during an appropriate technology refresh period
  - Transition milestones
  - Application Interoperability Planning (Block Transitions): There may be a need to transition enterprise applications in blocks for interoperability purposes.
  - COTS application transition schedules: Work with vendors to get realistic transition and availability schedules.
- **Training:** Needed training for application developers based on application types and development/testing environment.

- **Application Laboratory:** Consider developing or utilizing an application development laboratory for training, developing, and test activities.
- **Application Testing:** Test application in laboratories, pilots, and actual operational conditions.
- **Application Transition Guidance:** Develop comprehensive guidance for developers for transitioning applications to IPv6. In order to be considered “fully dual stacked” all applications functions requiring IP connections should be able to operate in either an IPv4-only mode or an IPv6-only mode, to include all calls to external applications such as DNS, RPC, and software update functions. Any IPv6 application with dependencies on IPv4 functions should be considered “partially dual stacked” and the dependencies noted.
- **Subtle IPv6 Application Programming Issues to Consider:**
  - IPv6 address nomenclature
    - Colon Separators
    - Hexadecimal Addresses
  - Protocol Data Structures for storing Dual Stack information and 128-bit address fields
  - Application Logic for Protocol Selection
  - Protocol Defaults
  - Fixed IP addresses
  - Port utilization
  - Security features
  - Changes to Socket and Advanced-Socket function calls
  - Incorporation of new IPv6 features
  - GUI design for IPv6
  - Network management and security applications are heavily tied to IP addressing and features and are especially difficult to port to a completely new version of IP
  - Data structure, record, and field widths for IPv6 addresses
  - Data rate and latency variations

The USG IPv6 Profile also has a section on application considerations for IPv6 and what it might mean to produce an IPv6-enabled application. The Profile can be found at <http://www.antd.nist.gov/usgv6/usgv6-v1.pdf>).

### 5.2.8 IPv6 Desktop Access

There are two primary IPv6 desktop access considerations:

- **Managed Tunnels (VPN):** Future purchases of VPN and remote access clients and servers should include the ability to connect over IPv4 or IPv6.
- **Virtual Desktops:** Virtual desktop servers and clients should be able to connect over IPv4 or IPv6. Remote virtual desktop sessions being served external to the Enterprise should be protected utilizing strong cryptography: IPsec, SSL, or application layer security.

## 5.3 Security

Agencies must evolve their IT security policies and architectures to take into account new capabilities that will be required within IPv6, but also to take advantage of some of the inherent security-related features available within IPv6. Implementing IPv6 within an IPv4 network effectively creates a dual network layer, which inherently increases exposure to attacks. While many attack strategies for IPv6 may mimic known IPv4 attacks such as sniffing, man-in-the-middle, flooding, application layer attacks and rogue devices, new forms of attack are likely. For example, many IPv4-IPv6 co-existence technologies utilize tunnelling which requires deeper packet inspection capabilities to scan tunneled packet information.

Because production network experience with IPv6 and its resilience to attack is currently limited, proactive steps are necessary to minimize exposure. Security monitoring tools, perimeter gateway systems, remediation systems, processes and infrastructure and host security measures need to be tested and qualified in terms of IPv6 protocol support and attack detection and remediation capabilities. Network security personnel need to be trained on IPv6 protocol operation, including its security benefits as well as potential vulnerabilities. Security vulnerability detection and reporting sources such as the US-CERT must be monitored regularly for current vulnerability reports to rapidly assess and mitigate relevant vulnerabilities.

Avoiding these steps or IPv6 in general is not a viable security solution. Even if an agency does not activate IPv6, they will nonetheless not be immune from IPv6 security issues. In some cases, devices within the agency's network may be IPv6-operational by virtue of their default configuration without the agency's knowledge. These devices could for example utilize tunneling technology to reach across the agency's current network to the Internet.

The following is a non-exhaustive list of possible attacks and suggested mitigation practices that require consideration when implementing IPv6.

- **Reconnaissance:** Unauthorized identification and mapping of network topology.
  - The large interface ID field within each IPv6 address makes traditional network layer address scans difficult though not entirely impossible (assuming 64 bit subnet identifier and good IPv6 address selection techniques)
  - Filter internal-use multicast addresses (e.g. by site, organizational scope)
  - Consider implementation of privacy extensions for interface IDs
  - Filter internal-use (e.g. unique local) IPv6 addresses at border

The IPv6 transition at the Department of Veterans Affairs (VA) is not just a "network only change" - but a change that would impact every aspect of the VA Enterprise that utilizes the network for communications.

During planning for the IPv6 transition, the VA took the following steps:

- Identify assets ;
- Identify vulnerabilities ;
- Identify threats;

- Determine the effects of the threat-to-vulnerability ratio;
- Prioritize high risks;

- Accept, transfer, or mitigate the high-priority risks;

The VA also developed a comprehensive IPv6 training program and awareness video, currently available at: (<http://www.gsa.gov/Portal/gsa/>). The VA is currently developing an updated video due in March 2009.

- Use “non-obvious” static IPv6 addresses for critical systems; i.e. don’t increment beginning at 1 on a subnet.
  - Filter unneeded services at the firewall and selectively filter Internet Control Message Protocol (ICMP)
  - Maintain host and application security
- **Unauthorized Access:** Inappropriate access on a node to applications or upper-layer protocols.
  - Utilize traditional filtering/firewall technology but update for IPv6, ICMPv6, and tunneling inspection
  - IPv6 adds the ability to utilize multiple addresses per interface for greater filtering capabilities
  - IPv6 extension headers may be an issue (e.g. Type [0] routing header) and should be considered and incorporated into the security strategy
  - Update firewall for anycast and ICMPv6 inspection
  - Enforce multicast packet scoping; i.e., prevent multicast packets from being forwarded beyond the specified scope (e.g., local, site, organizational, etc.)
  - Implement application layer security as well; e.g. secure access, identity management, SSL, etc.
- **Header Manipulation and Fragmentation:** Modification of IP header or use of fragmentation to evade security devices or attack the network infrastructure.
  - Deny IPv6 fragments to an internetworking device if possible
  - Drop fragments of less than 1280 octets, the minimum MTU
  - Apply filtering rules if IPv4-IPv6 translation technologies in use
- **Layer 3 and Layer 4 Spoofing:** Modifications to packets to allow attackers to appear to be coming from a different location and/or for another application.
  - Develop last hop IP trace-back capability
- **Dynamic Host Configuration Protocol (DHCP) Attacks:** Providing false information during a device initialization process with the network.
  - Look at layer 2 authentication mechanisms such as 802.1x
  - Filter DHCP solicits by a “known list” of device unique IDs (DUIDs)
- **Broadcast Amplification Attacks (smurf):** Denial of service attack where other nodes on a subnet are tricked into flooding packets to a single node on the subnet.
  - Properly implemented IPv6 stacks will not be susceptible to this attack so testing this attack should be part of IPv6 stack testing
  - Filter packets with a source multicast address
- **Routing Attacks:** Disrupts network routing flows or makes unauthorized changes to the routing tables.

- Many routing protocols did not make changes in security to support IPv6; however, some have dropped authentication capabilities in expectation of utilizing IPsec
- Use existing authentication mechanisms for BGP and IS-IS
- Use IPsec with OSPFv3 and RIPng
- **Viruses and Worms**
  - Viruses and worms that rely on network scanning techniques will be limited in their attack capabilities
- **Transition Mechanisms:** Tunneling and translation techniques utilized to support coexistence of IPv4 and IPv6 on the same infrastructure.
  - Establish clear security policies with regard to tunneling
  - Filter rogue tunnels at the firewalls or routers
  - Use state tunnels or automated tunneling mechanisms that provide authentication mechanisms and have greater administrative control

In summary, agencies need to consider the following with regard to security:

- Develop a comprehensive IPv6 security plan and associated IPv6 policies within the IPv6 addressing rollout plan
- Routers/switches
  - Disable IPv6/tunnels unless and until required by the IPv6 addressing and security plans.
  - Implement Access Control Lists (ACLs) to block IPv6 traffic and/or tunnels on core/edge/outside perimeter unless and until required by the IPv6 addressing and security plans.
- Upgrade network protection devices/tools for IPv6 support
- Enable IPv6 IDS/IPS features
- Enable IPv6 host firewalls on all end devices
- Disable IPv6 on routers, infrastructure devices, servers and hosts unless and until required by the IPv6 addressing and security plans.
- Expand core and perimeter boundary monitoring to incorporate IPv6 and IPv6-in-IPv4 tunnels

## 5.4 Additional Tips

- **Integration of IPv6 in product lifecycle replacement (refresh cycles):** Enterprises are focusing on IPv6 migration cost reduction by adding it into the planned product procurements of their existing information technology budgets. If the enterprise IT staff includes upgrades to IPv6 as part of their regular procurement process and select IPv6-enabled products, they can take an evolutionary approach towards adoption of the new protocol.
- **Specifying IPv6 compliance in Requests for Proposals (RFPs):** Adding IPv6 support to new procurement beyond the core network helps enterprises meet the internal adoption deadlines for transition to IPv6. It refers to including the IPv6 support to all the IT requests for proposals. Integrating IPv6 procurement planning and training into existing IT processes helps the enterprises in meeting their upgrade deadlines while avoiding any unexpected or unnecessary costs.
- **Using transition technologies:** Enterprises are incorporating temporary network tunneling until the end of the device lifecycle to meet internally defined IPv6 compliance deadlines. Tunneling refers to the process of routing the IPv6 data packets through virtual paths in the network backbone by including them inside the IPv4 network address headers. Prior to the delivery at the node, the IPv6 packets are extracted and delivered via IPv6 service.
- **Integration of IPv6 training into IT budget:** Training costs might be significantly high in cases of IPv6 migration. Integration of IPv6 training costs into the IT training budget helps provide a smooth transition. Ideally, IPv6 should be considered a separate protocol requiring hands-on practice to gain proficiency.
- **Test with Simulation Tools:** IPv6 upgrades involve technology refresh that many federal network architects are unfamiliar with. The complex interaction of new network architectures and their impact on application performance make it impossible to reliably predict successful delivery of services to all users. Simulation or emulation-based pre-deployment testing of systems of new record and applications under real world scenarios would mitigate this risk and insure a higher degree of continuity of operations and end user satisfaction.

Some of the drivers that helped move Department of Transportation (DOT) towards the implementation of IPv6 were the building of a new headquarters building, looking at the future of technology and how the Federal government needs to help move technology forward. DOT not only explored the use of IPv6 in the support of its infrastructure, but also in the development of major programs, such as the Intelligent Transportation System (ITS) and Next Generation Air Transportation System (NGATS) to pave the way towards improved roads and reduced congestion.

Achievements include the implementation of IPv6 across the core of the campus network and plans to complete the implementation of IPv6 across the entire WAN as communication service providers become capable of the supporting IPv6.

## Section 6:

## IPv6 Impact on Federal Initiatives

The USG has numerous federal-wide initiatives underway to improve the overall security and operability of the federal enterprise architecture as well as limit or reduce cost. Figure 9 depicts a number of initiatives that may appear to be separate, but are intricately linked. Many agencies are tackling these initiatives in a silo fashion and do not fully understand how each are related and will ultimately impact new “to be” architectures being developed.

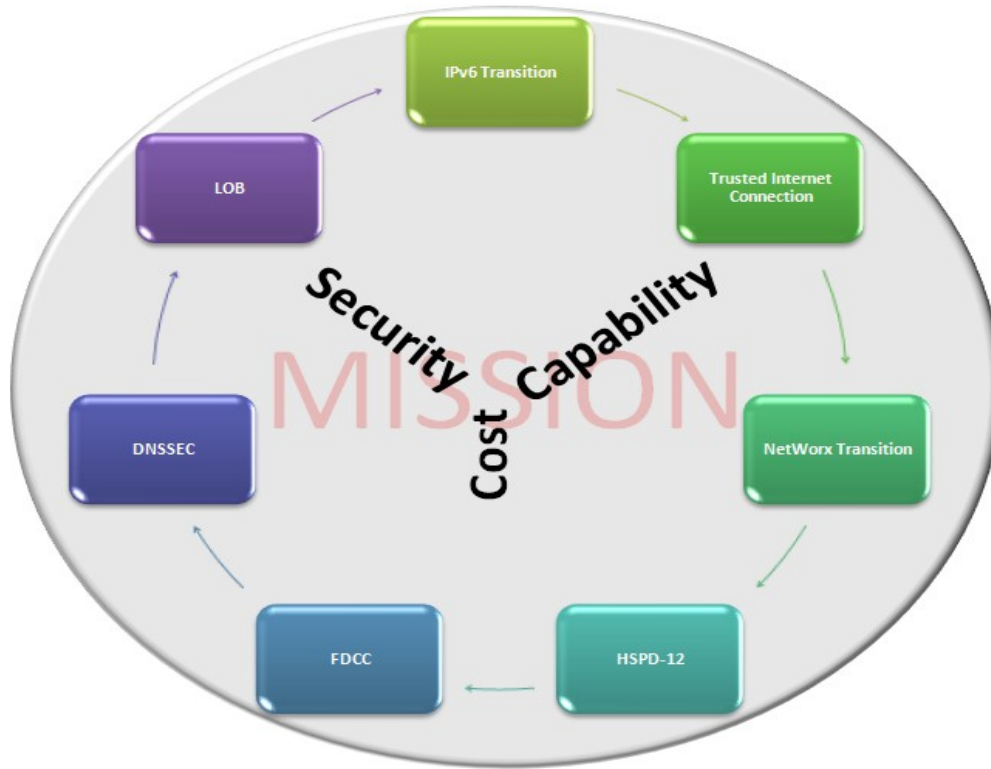


Figure 9 – IPv6 Relation to Other Federal Initiatives

This section examines the potential IPv6 related impacts agencies should consider when developing their solution sets for each of these initiatives. In reality, agencies need to look at the initiatives in a coordinated fashion and understand the cross-requirement impacts that will occur as individual solution sets are developed.

The development of solution sets and “to be” architectures for each of these efforts in a silo methodology will lead agencies to developing solutions sets that will potentially be conflicting or counterproductive. In addition, Trusted Internet Connections (TIC) may not support other efforts that could be directly impacted.

In order to utilize their resources most efficiently, agencies need to consider working these efforts in unison. This will ensure that requirements which impact more than one initiative are taken into account across the board and that complimentary solutions are developed as a part of the solution process.

## 6.1 TIC

Trusted Internet Connections (TIC) is a major federal initiative focused on developing a more secure boundary between the entire Federal Enterprise Architecture (FEA) and the surrounding world. TIC focuses on bringing all external IP-based connections through a limited number of gateways which have access into federal agencies. This solution provides greater control and an increased ability to monitor connections. As agencies move to implement both TIC and IPv6, there will be significant overlaps in requirements that should be addressed during the planning cycles for both. IPv6 will directly impact many of the short and long-term TIC solutions. Agencies must consider the following areas:

- IPv6 policy
- IPv6 routing/traffic
- IPv6 DNS
- IPv6 firewall functionality
- IPv6 IDS capability
- Support for IPv6 based IPsec
- IPv6 tunneling
- IPv6/IPv4 translation
- IPv6 privacy/address hiding
- IPv6 network management

If an agency has sites at different geographic locations that require multi-homed ISP service at varying TIC connection points, their IPv6 addressing should be from a block large enough to divide it into multiple subnets that can be advertised across different TIC service providers. The digital certificates used in HSPD-12 should have the ability to store IPv6 addresses associated with the certificate. As with IPv4 addresses, this is not a requirement but is a capability that should be supported. See *NIST "Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile"*, dated October 12, 2005 for additional information.

## 6.2 HSPD-12

Homeland Security Presidential Directive 12 (HSPD-12) was issued in August 2004 to improve the security of federal facilities and information systems by implementing common processes for identity proofing and ensuring interoperability through use of standardized credentials for physical and logical access.

While tying identification of users to electronic assets can be implemented independent of the TCP/IP layer, agencies should also consider how IPv6 could support greater usability and capabilities of their HSPD-12 implementations to support IPsec authentication and encryption services. All federal employees and contractors will receive HSPD-12 credentials, and agencies can use these credentials as the encryption key.

Some agencies have started exploring the use of IPv6 addresses coupled with their HSPD-12 implementation to develop a more robust and scalable security architecture that can provide a service-oriented architecture (SOA) approach to lower the cost of future security requirements.

As agencies prepare their implementation plans, they should take into account areas that may impact or provide future benefits, including:

- The use of multiple IPv6 addresses to support compartmentalization
- The use of common digital certificates/PKI system to support HSPD-12 functionality and IPsec
- Geospatial functionality using IPv6 for location-based services
- Common security identification and authentication from an IP layer

### **6.3 IT Infrastructure Line of Business (ITILoB)**

The IT Infrastructure Line of Business which emphasizes the measurement of outcomes for infrastructure improvements was recently started by OMB and is being managed by GSA. The scope is all Federal IT commodity services including data centers, data networks and telecommunications, and desktop / seat management and support. As this line of business moves forward, IPv6 will have a major impact on the overall initiatives. Agencies should coordinate and include their IPv6 transition activities within the scope of this LOB. In particular, GSA and agencies should identify:

- Common IPv6 solutions that may be applied cross-agency
- Ability to develop and implement common IPv6 based services that may support multi-agency implementations
- Lessons learned and best practices
- Cross-agency common purchasing agreements based on the NIST IPv6 profile
- Common solution sets for security and IPsec functionality to support cross-agency security functionality

### **6.4 FDCC**

Commercial deployment of IPv6 on standard operating systems (OS) has progressed rapidly. Almost every current major commercial OS has IPv6 embedded within it. In some cases, IPv6 is active by default and may be required to support certain applications.

As agencies develop their desktop requirements to meet the Federal Desktop Core Configuration (FDCC), they must understand the IPv6 requirements that should be taken into account. This should include policy, default configurations and settings, and IPv6 security capabilities as well as other potential requirements regarding IPv6.

Agencies should consider the following potential IPv6 impacts when developing their FDCC solutions:

- Remote access requirements
- Virus and firewall scanning capabilities
- Support for centralized management
- Default configuration settings

### **6.5 Network Migration**

Transitioning to Network will be one of the greatest opportunities for agencies to implement IPv6 across their entire enterprise in a cost-effective manner. As agencies develop their Network

requirements, they should do so in conjunction with their short and long-term IPv6 plans to ensure that their Networkx vendor will adequately support their requirements. This should include every aspect of the enterprise that is being impacted during the Networkx transition and not just the core network. Even if agencies are not planning on using the IPv6 functionality initially, having it in place and supported under the initial transition can save significant costs and resources down the road. In addition, it will allow agencies to respond faster to changing market conditions and utilize new IPv6 capabilities that can drive a positive return on investment.

During their Networkx transition planning efforts, agencies should consider the following potential IPv6 impacts:

- IPv6 routing
- IPv6 addressing
- IPv6 multi-homing/business continuity
- IPv6 security (firewall/IDS)
- Telework/remote access
- IPv6 device management
- IPv6 network management
- IPv6 SLAs
- DNS support

## **6.6 DNSSEC**

Adding Domain Name System Security Extensions (DNSSEC) cryptographic authentication services to DNS servers by December 2009, as required by OMB M-08-23 memorandum, will be combined with a requirement to serve IPv6 AAAA records.

## Section 7:

# IPv6 in IT Governance and Procurement

One of the most difficult aspects of any technology transition is the policy and procurement phase. Agencies need to understand their overall top-down approach to transitioning to IPv6 and ensure that it is correctly supported in their policies as well as their government and procurement programs.

### 7.1 Governance

Agencies will need to update their Transition Strategy Plans plans to reflect the next steps in their IPv6 transition. This needs to be done in lock-step with the release of new agency policy and procedures that will continue to support the orderly transition to IPv6. In addition, agencies should review their IPv6 transition teams to ensure that as their goals evolve over time, their roles and success metrics change to match the new goals. In addition, senior-level support is needed in the on-going transition to ensure agency-wide participation.

Agencies should:

- Develop updated policies to support the on-going IPv6 transition activities to include:
  - Stated organizations objectives
  - Capabilities based on stated milestones
  - Required advanced IPv6 features
  - IPv6 functional hurdles
  - Definition of IPv6-capable
  - Program preparation and planning requirements
  - Locations for deployment
  - Levels of security
  - Utilization of IPv6
  - Functional profiles
  - Prohibitions of use
- Develop milestones that are believable and achievable
- Publish guidelines for minimum functional capabilities by specific milestones
- Point to a technical architecture
- Establish an agency plan and schedule
- Inject IPv6 into current programs and projects

### 7.2 Procurement

One of the primary tenets associated with the federal IPv6 transition philosophy has been the use of technology refreshment cycles to enable IPv6 across the FEA. This concept supports an extended transition timeframe where agencies can incorporate IPv6 into their normal acquisition cycles over time; thus alleviating large capital deployments to support the transition. In accordance with Federal Acquisition Regulation (FAR) 11.002(g), agencies need to include the

appropriate standards for IPv6 in all IT related acquisitions that have any relation to the network. In addition, agencies must review the NIST IPv6 Product Profile and Testing plans to determine how to specify future IPv6 product acquisitions.

Agencies should consider:

- FAR-compliant acquisition and procurement language for all IT-related products and services
- Development of standard contractual language
- Investigate the modification of past contractual language
- Consider issuing an IPv6 contractual vehicle that permits all agency entities to contract for IPv6 support
- Develop product profiles based on the recently released NIST IPv6 Product Profile

**Section 8:**

**Acronym Dictionary**

| Acronym                 | Description  |
|-------------------------|--|
| <b>AAAA</b>             | Authentication, Authorization, Accounting and Auditing   |
| <b>ACL</b>              | Access Control List  |
| <b>ARIN</b>             | American Registry for Internet Numbers   |
| <b>ARP</b>              | Address Resolution Protocol  |
| <b>CCTV</b>             | Closed Circuit Television  |
| <b>CPIC</b>             | Capital Planning and Investment Control  |
| <b>COI</b>              | Communities of Interest  |
| <b>COOP</b>             | Continuity of Operations Plan  |
| <b>DHCPv6</b>           | Dynamic Host Configuration Protocol for IPv6   |
| <b>DISR</b>             | DoD Information Standards Registry   |
| <b>DMZ</b>              | Demilitarized Zone. A metaphor for network segments (more open to the public Internet than systems inside the enterprise but not entirely unprotected) on the external edge of an enterprise.  |
| <b>DNS</b>              | Domain Name System   |
| <b>DNSSEC</b>           | Domain Name System (DNS) Security Extensions   |
| <b>DoD</b>              | Department of Defense  |
| <b>DOT</b>              | Department of Transportation   |
| <b>EA</b>               | Enterprise Architecture  |
| <b>EAAF</b>             | Enterprise Architecture Assessment Framework   |
| <b>E-Authentication</b> | Electronic Authentication  |
| <b>e-Gov</b>            | Electronic Government  |
| <b>E-Mail</b>           | Electronic Mail  |
| <b>ESP</b>              | Encapsulating Security Protocol  |
| <b>FDCC</b>             | Federal Desktop Core Configuration   |
| <b>FEA PMO</b>          | Federal Enterprise Architecture Program Management Office  |
| <b>FTP</b>              | File Transfer Protocol   |
| <b>GRE</b>              | Generic Routing Encapsulation  |
| <b>HSPD-12</b>          | Homeland Security Presidential Directive (HSPD) 12 is "Policy for a Common Identification Standard for Federal Employees and Contractors"  |
| <b>HSPD-20</b>          | Homeland Security Presidential Directive (HSPD) 20 is sometimes called simply "Executive Directive 51" (for short). The Presidential Directive specifies the procedures for continuity of the federal government in the event of a "catastrophic emergency". Such an emergency is construed as "any incident, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the U.S. population, infrastructure, environment, economy, or government functions." |
| <b>IA</b>               | Information Assurance  |
| <b>IKE</b>              | Internet Key Exchange  |
| <b>IP Fax</b>           | Internet Protocol Facsimile  |
| <b>IPS</b>              | Intrusion Prevention System  |
| <b>IPSec</b>            | Internet Protocol Security   |
| <b>IPT</b>              | Internet Protocol Telephony  |
| <b>IPv4</b>             | Internet Protocol Version 4  |
| <b>IPv6</b>             | Internet Protocol Version 6  |
| <b>ISATAP</b>           | Intra-Site Automatic Tunnel Addressing Protocol  |
| <b>ISP</b>              | Internet Service Provider  |
| <b>IT</b>               | Information Technology   |
| <b>ITI LoB</b>          | Information Technology (IT) Infrastructure Line of Business  |
| <b>ITI PPMO</b>         | IT Infrastructure Program Performance Measurement Office   |
| <b>LAN</b>              | Local Area Network   |
| <b>LoB</b>              | Line of Business   |
| <b>MAC ID</b>           | Media Access Control Identification. MAC is also known as Medium Access Control  |

# Appendix A: Guide to Incorporating IPv6 into IT Infrastructure Segment Architectures

*Excerpt from NIST Special Publication 500-267 - “A Profile for IPv6 in the U.S. Government – Version 1.0”*  
(<http://www.antd.nist.gov/usgv6/usgv6-v1.pdf>):

Serious planning for IPv6 adoption in existing, or planned, IT systems is a very complex undertaking. The issues range from incremental deployment plans for new IPv6 data and control plane protocols, to coexistence and interoperation plans for existing IPv4 based infrastructure, to security and management plans for the resulting IPv6 (and mixed IPv4) infrastructure. Certainly a key factor in planning for IPv6 is the extent to which it must coexist and interoperate with an existing IPv4 infrastructure.

The first step towards the successful adoption and widespread use of IPv6 is the establishment of a core network infrastructure capable of providing IPv6 data services to the applications that will eventually follow. Establishing an IPv6 core network infrastructure opens the door to creating new host applications adapted to exploit the added capabilities of the new infrastructure. It is exactly this potential, to develop new applications, at larger scales, that is the real, long-term promise of IPv6. This profile provides the minimal mandatory definition of an IPv6 Host

The following documents that address many of these issues in specific deployment and transition scenarios:

- **Enterprise Networks:**

1[RFC4057] *IPv6 Enterprise Network Scenarios.*

2[RFC4852] *IPv6 Enterprise Network Analysis - IP Layer 3 Focus.*

3[RFC3750] *Unmanaged Networks IPv6 Transition Scenarios.*

4[RFC3904] *Evaluation of IPv6 Transition Mechanisms for Unmanaged Networks.*

5

- **ISPs and Transit Network Infrastructure:**

6[RFC4029] *Scenarios and Analysis for Introducing IPv6 into ISP Networks.*

7[RFC2185] *Routing Aspects of IPv6 Transition.*

8

- **Interoperation with IPv4 Infrastructure:**

- 9[RFC4038] *Application Aspects of IPv6 Transition.*
- 10[RFC4213] *Basic Transition Mechanisms for IPv6 Hosts and Routers.*
- 11
- **Security Issues:**
- 12[RFC4942] *IPv6 Transition/Co-existence Security Considerations.*
- 13[RFC4864] *Local Network Protection for IPv6.*

## 1.0 Business Architecture

Using the table below, please define network services/capabilities that support your Agency’s core mission applications.

| Core Mission Applications | Segment Architecture | Network Services Required |
|---------------------------|----------------------|---------------------------|
|                           |                      |                           |
|                           |                      |                           |
|                           |                      |                           |

Listed below are examples of network services/IPv6 Capabilities that may be used to support your core mission applications. Please note that this is not an exhaustive list but should be used for guidance.

Each of the network services/IPv6 capabilities listed is mapped to a Functional Category specified in NIST Special Publication 500-267 - “A Profile for IPv6 in the U.S. Government – Version 1.0” (<http://www.antd.nist.gov/usgv6/usgv6-v1.pdf>).

| Functional Category     | Notes - Examples   |
|-------------------------|--|
| IPv6 Basic Capabilities | IPv6, ND, SLAAC, DHCP, FTP, DNS, E-mail, Printing, Network file system, Browsing (HTTP/HTTPS), Internet Information Services, Directory services |
| Routing Protocols       | OSPF, BGP  |
| Quality of Service      | DiffServ   |
| Transition Mechanisms   | Dual Stack, Tunneling, 6PE   |
| Link Specific           | IP over X, ROHC  |
| Addressing              | IPv6 global, ULA, CGA  |
| IP Security             | IPsec, IKE, Cryptographic Algorithms   |

| Functional Category                    | Notes - Examples   |
|--|--|
| Network Management                     | SNMP, MIBs   |
| Multicast                              | MLDv2, PIM-SM  |
| Mobility                               | MIP, Nemo, Voice over Internet Protocol (VoIP) Transport Services, Internet Protocol Telephony (IPT) Services, Internet Protocol Facsimile (IP Fax) Services, Internet Protocol Video Transport, Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metro Area Network (WMAN), and Wireless Wide Area Network (WWAN) technologies, Instant Messaging Services, Unified Messaging Services, Radio over IP, Video Conferencing, TeleWork: <ul style="list-style-type: none"> <li>– Premise-based Virtual Private Network (VPN) services</li> <li>– Network-based VPN Services</li> <li>– Audio, video and data communications</li> <li>– Managed notebook/desktop support services</li> <li>– Security services</li> <li>– Application support through the Systems/Data Center services</li> <li>– Customer support services through the Helpdesk and Desktop services</li> </ul> |
| Application Requirements               | Sockets, DNS, URIs, guidance.  |
| Network Protection Device Requirements | Firewalls, intrusion detection systems, IPS  |
| Miscellaneous                          | E-Learning, Video Surveillance, Video On-Demand, Asset Tracking  |

## 2.0 Service Component Architecture

Please complete the following table to define the applications/devices providing each of the network services defined in your business architecture. It is recommended that you use the Application and Device Inventory completed by your agency in compliance with OMB Memorandum 05-22 as a starting point.

For each application/device, please:

- Determine what IPv4 address spaces are in use
- Inventory and baseline the associated Dynamic Host Configuration Protocol (DHCP) server configurations
- Identify and record associated Domain Name Server (DNS) configurations and resource records associated with IPv4 devices.

| Network Service | Application / Device Name | Refresh Date | Device Capability (IPv4, IPv6, Dual Stack) | IP Address(es) Used* | DHCP Server Configurations | DNS Server Configurations |
|-----------------|---------------------------|--------------|--|----------------------|----------------------------|---------------------------|
|                 |                           |              |  |                      |                            |                           |
|                 |                           |              |  |                      |                            |                           |
|                 |                           |              |  |                      |                            |                           |

\* There may be multiple addresses IP addresses for a network service.

## 2.1 IPv6 Addressing Changes

Please use this section to identify IP Addressing Change Requirements.

| Network Service | Application / Device Name | IPv4 Subnet Address | IPv6 Subnet Address |
|-----------------|---------------------------|---------------------|---------------------|
|                 |                           |                     |                     |
|                 |                           |                     |                     |
|                 |                           |                     |                     |

## 3.0 Technical Architecture

Please use the following table to define the technical components of each Application/Device.

| Application/Device Name           | FEA TRM Service Area | FEA TRM Service Category | FEA TRM Service Standard | Service Specification |
|-----------------------------------|----------------------|--------------------------|--------------------------|-----------------------|
| <b>IPv4 Capability Only</b>       |                      |                          |                          |                       |
|                                   |                      |                          |                          |                       |
|                                   |                      |                          |                          |                       |
| <b>IPv6/Dual Stack Capability</b> |                      |                          |                          |                       |
|                                   |                      |                          |                          |                       |

## 4.0 Security

Please use the following table to define the security capability and specifications needed for each application/device and network Services

| Application/Device Name | Network Service | Security Capability Needs | Security Specifications |
|-------------------------|-----------------|---------------------------|-------------------------|
|                         |                 |                           |                         |
|                         |                 |                           |                         |

## 5.0 Transition Milestones

1. Please describe your plans and target dates for establishing an IPv6 Test Lab:
2. Because of IPv4 address depletion and its affect on core routing, it is recommended that
  - a) Applications that rely on the Internet core for transport to external hosts should upgrade first to IPv6-capable versions by 2010.
  - b) Upgrade host interfaces such as Web servers and e-mail clients that will have to connect to external servers.
  - c) Upgrade internal facing systems in an Enterprise LAN should come as a third priority, as these systems can continue to rely on IPv4 NAT addresses for some time.

Since sites will transition to IPv6 in a phased approach, the best plan forward for web servers is to simply enable dual-stack addressing with both IPv4 and IPv6 addresses and ensure that there is either a native or tunneled IPv6 path between all IPv6 clients and the servers. Web servers should have both their IPv4 and IPv6 addresses configured into DNS servers.

Please provide your plans for completing these milestones in the table below:

| Milestone   | Agency Plan | Anticipated Completion Date |
|---|-------------|-----------------------------|
| Applications that rely on the Internet core for transport to external hosts should upgrade first to IPv6-capable versions by 2010 |             |                             |
| Upgrade host interfaces such as   |             |                             |

| Milestone  | Agency Plan | Anticipated Completion Date |
|--|-------------|-----------------------------|
| Web servers and e-mail clients that will have to connect to external servers   |             |                             |
| Upgrade internal facing systems in an Enterprise LAN should come as a third priority, as these systems can continue to rely on IPv4 NAT addresses for some time. |             |                             |

3. Please specify other IPv6 Transition Milestones – including those for upgrading IPv4 only capable devices and deploying IPv6-enabled network services.

| Network Service | Application/Device Name | Target Deployment Date | Implementation Milestones | Requires TRM/Technology Update? If so, Please Specify? | IPv6 Device Configuration Strategy? (stateless autoconfiguration, stateful configuration or hybrid) | Target Milestone Date |
|-----------------|-------------------------|------------------------|---------------------------|--|---|-----------------------|
|                 |                         |                        |                           |  |   |                       |
|                 |                         |                        |                           |  |   |                       |

## References

- <sup>1</sup> The Council of the European Union, "Council Conclusions on Future Networks and the Internet", December 1, 2008. [http://ec.europa.eu/information\\_society/eeurope/i2010/key\\_documents/index\\_en.htm#i2010\\_High\\_Level\\_Group\\_discussion\\_papers](http://ec.europa.eu/information_society/eeurope/i2010/key_documents/index_en.htm#i2010_High_Level_Group_discussion_papers)
- <sup>2</sup> Huston, Geoff. APNIC 24 Plenary Session: "The Future of IPv4," September 2007. [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_10-3/103\\_addr-dep.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-3/103_addr-dep.html).
- <sup>3</sup> Mosquera, Mary, "OMB: Agencies met IPv6 deadline," July 1, 2008. <http://www.fcw.com/online/news/153018-1.html>.
- <sup>4</sup> Jackson, William, "IPv6 standards profile released," September 19, 2008. [http://www.gcn.com/online/vol1\\_no1/47182-1.html?page=2](http://www.gcn.com/online/vol1_no1/47182-1.html?page=2).
- <sup>5</sup> National Institute of Standards and Technology, "NIST Special Publication 500-267: A Profile for IPv6 in the U.S. Government – Version 1.0", July 2008. <http://www.antd.nist.gov/usgv6/usgv6-v1.pdf>.
- <sup>6</sup> Practical Guide on Federal Service Oriented Architecture, June 2008. <http://smw.osera.gov/pgfsoa/index.php/Welcome>
- <sup>7</sup> The Open Group, "Service-Oriented Infrastructure Project Description", July 31, 2007. <http://www.opengroup.org/projects/soa-soi/doc.tpl?CALLER=index.tpl&gdid=14171>
- <sup>8</sup> Improving Agency Performance Using Information and Information Technology, Enterprise Architecture Assessment Framework (EAAF) version 3.0. December 2008. <http://www.whitehouse.gov/omb/e-gov/fea/>