Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government

Strategy and Planning Committee
Federal Chief Information Officers Council

Version 2.0
July 2012

**The Federal CIO Council Strategy and Planning Committee
Technology Infrastructure Subcommittee
Federal IPv6 Working Group**

In collaboration with the

**The American Council for Technology/Industry Advisory Council's
Network and Telecommunications (N&T-SIG)**

Present:

Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government

July 2012

Table of Contents

List of Exhibits

Executive Summary

The Internet is changing. The current network protocol, Internet Protocol, version 4 (IPv4), has reached the end of its life, and to maintain connectivity with its constituents the United States (U.S.) Federal Government must provide leadership on the process of evolving to the next Internet Protocol, version 6 (IPv6). The current Federal efforts were established to ensure the Federal Government's business continuity as the legacy Internet based on IPv4 can no longer expand to meet demand. On February 3rd 2011, the last available IPv4 addresses were released regionally for consumption. The Asia Pacific region exhausted its supply in April 2011, and the European and North American region's supplies are projected to follow shortly.

However, there is more to the IPv6 transition than achieving the basic objective of providing additional addresses. As Federal agencies integrate IPv6 within their current operations, they also have the opportunity to employ the new technology to optimize and enhance their business functions. The technological advances provided by the new protocol will enable agencies to significantly enhance their mission capability by removing the limiting technology of the legacy protocol, IPv4, and adopting IPv6 as the new standard for supporting operational efficiency.

The Federal Government has long recognized the importance of the transition to IPv6. In August 2005, the Office of Management and Budget (OMB) issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)" requiring the deployment of IPv6 on Federal Government network backbones by June 2008. While Federal agencies have achieved the objectives of that directive, feedback from the Departments indicated that continued adoption of IPv6 within Federal enterprises required additional guidance.

Accordingly, the Federal Chief Information Officers (CIO) Council took action to develop and issue well-defined private/public best practices guidelines in the initial "Planning Guide/Roadmap toward IPv6 Adoption within the U.S. Government" (the "Roadmap") released in May 2009. Given the technical complexities involved with full enterprise transitions, as well as the fast approaching world-wide exhaustion of IPv4 addresses, OMB released a subsequent memorandum (entitled "Transition to IPv6") in September of 2010. This memorandum stipulated enterprise goals and deadlines for all Federal agencies and referenced the May 2009 Roadmap as the foundational planning document for use by all agencies.

This document is the latest version of the Roadmap, and is the key guidance document for supporting Federal agencies in their achievement of the 2012 and 2014 objectives, as well as the strategic vision for beyond 2014. This document has the same foundational elements instituted in the original Roadmap, and has been updated to reflect the three years of experience (from both the public and private sectors) since original publication. The sections of the document comprise all aspects of a successful transition and now include practical experience from those directly engaged in IPv6 activities, combining programmatic (including Clinger-Cohen Act compliance), technical, cybersecurity, and Federal acquisition elements, as well as the suggested interactions with other Federally mandated technical efforts such as the Trusted Internet Connection (TIC).

1. Introduction

The U.S. Federal Government is engaged in the effort to sustain its Internet connectivity with its constituents and business partners (both public and private) as the Internet evolves to the next Internet Protocol, version 6 (IPv6). The "Transition to IPv6" directive issued on September 28th, 2010 by the Federal CIO is intended to ensure the Federal Government's business continuity since the legacy Internet can no longer expand to meet demand. The directive's phased objectives, set respectively for end of FY2012 and FY2014, allow the appropriate resources to be brought to bear to accomplish the objectives, but there is more to be gained than simply achieving the objective of providing additional IP addresses. As Federal agencies integrate IPv6 within their current operations, they also have the opportunity to employ the new technology to optimize and enhance their business functions. The technological advances provided by the new protocol enable agencies to significantly enhance their mission capability by removing the limiting technology of the legacy protocol, IPv4, and adopting IPv6 as the new standard for supporting operational efficiency.

The purpose of this Roadmap is to provide Federal Government agency leaders with practical and actionable industry and Federal agency best practices guidelines on how to successfully integrate IPv6 within their enterprises. The Roadmap has been updated from the original published in 2009 to provide the Federal Government's IPv6 history, vision, current goals, and deadlines. Based on the information provided in this document, agency Chief Information Officers (CIO), IPv6 Transition Managers, Chief Enterprise Architects, and Chief Acquisition Officers (CAO) should assess their agency's progress towards IPv6 adoption. This includes critical assessment of their current plans and planning efforts in meeting the FY2012 and FY2014 objectives.

1.1   Background

Businesses have embraced the Internet in order to increase the variety of services offered and to reduce the cost of providing these services to growing numbers of customers. The current Internet is a commercialization of a U.S.-funded (Defense) Advanced Research Project Agency (ARPA) project that began in the 1960's and is a key source of technological leadership as well as humanitarian and economic benefit to the United States and the world. The protocol that established the current Internet is IPv4 which only has 4.3 billion addresses.

In the mid to late 1990s, after thirty years of meteoric Internet growth, a major technology refresh was developed and deployed for the underlying communications technology of the Internet and the World Wide Web (www). This included implementation of high-speed fiber optic communications links transmitting data at speeds of over one terabit per second (Tbps). High speed routers and switches are being deployed to route, switch and deliver data to large virtualized data centers and high speed consumer, business, and government networks. These systems are capable of handling electronic traffic for hundreds of millions to billions of attached devices. Currently, the number of wireless devices connected to the network has exceeded one billion.

In the same timeframe the Internet community in cooperation with U.S. and other governments, began developing the required protocol components of the Next Generation Internet Network protocol, IPv6. One of the underlying reasons for the development of IPv6 was the projected exhaustion of the 4.3 billion IPv4 addresses. Due to the economic demand of greater "information accessibility" across the Internet, a high performance infrastructure is being deployed very aggressively to meet data and mobile computing requirements, while the deployment of the IPv6 protocols has not kept pace. For this Next

Generation "Super" Internet to operate effectively and reliably, while serving the ever expanding customer base, the IPv6 protocol must be universally implemented to allow the functional growth of the Internet as we know it. The current Internet has brought tremendous humanitarian, open government and economic benefit; it is in the best interests of the United States to continue to grow, support and expand these systems in order to provide increased connectivity and thus benefits.

Currently both IPv4 (the legacy version of IP) and IPv6 are being used on the Internet, but IPv4 is, by far, still the dominate protocol because of its legacy deployment. IPv6 traffic growth is inevitable due to the current state of IPv4 address exhaustion, creating an extreme supply and demand curve and required to support communications between the USG and its citizens and business partners worldwide. Agencies not only need to meet the 2012 and 2014 deadlines to achieve business continuity across the Internet, but they need to be able to leverage IPv6 protocol capabilities and ensure compatibility with new Internet services.

1.2   Adoption Benefits

The IPv6 protocol is the enabler of ultra-high performance networks providing for more efficient interconnection between bandwidth intensive Web and information services and their customers. The benefits of IPv6 include:

- Improves government operations for:
    - Streamlining services for more citizens and citizen groups
    - Improving of both the quality and delivery of Education and Healthcare in all areas of the country
    - Fostering environmental and energy monitoring and control
- Increases economic activity and increases jobs for urban and rural areas
- Supports remote and mobile offices and telework sites
- Fosters high speed equal Internet access for all
- Supports Continuity of Operations (COOP) for agencies

Some Federal initiatives supported include:

- "Cloud First" policy for secured Cloud Computing
- Federal Data Center Consolidation Initiative
- Transparent Government
- Digital Government Strategy

> **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.

1.3   Guidance

To address the impending exhaustion of the IPv4 address pool and in fostering these policies and benefits, on September 28, 2010, the Office of the Federal Chief Information Officer issued a Memorandum for Chief Information Officers of Executive Departments and Agencies, titled "Transition to

IPv6," which detailed the Federal Government's commitment to the operational deployment and use of IPv6. The memo states that OMB will work with the National Institute of Standards and Technology (NIST) to continue the evolution and implementation of the USGv6 Profile and Testing Program and provides guidance and deliverables agencies are required to achieve.

> "The US leadership is exemplary in this global undertaking. This is the first upgrade of the Internet and most probably the last one for decades to come. So, let's get it right."
>
> Latif Ladid
> IPv6 Forum President

1.4   Our Business Situation

Action is needed by the U.S. government in order to sustain our business continuity and retain our nation's technical and market leadership in the Internet sector thus expanding and improving services for America's citizens. Already, there has been significant progress by foreign governments to reap the advantages of early IPv6 deployment, including:

- **The European Commission**
  - i2010 initiative, an action plan to see IPv6 widely deployed in Europe by 2010
- **Australia**
  - A Strategy for the Implementation of IPv6 in Australian Government Agencies - July 2009
- **Peoples Republic of China**
  - Next Generation Internet project (CNGI), 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, using IPv6 to network everything from security cameras and taxis, to the Olympic events' cameras.
- **Hong Kong**
  - http://www.ogcio.gov.hk/en/business/tech_promotion/ipv6/ipv6_development_in_hk.htm
    A presentation at the IPv6 Transition Conference APRICOT-APAN 2011
    http://www.apricot.net/apricot2011/media/CK-Ng-APRICOT-APAN-HKG-IPv6.pdf
- **India**
  - The Government of India, Ministry of Communications and Information Technology, Department of Telecommunication's IPv6 Deployment Road Map, includes policy for:
    - All major service providers (having at least 10,000 Internet customers or STM-1 bandwidth) will target to handle IPv6 traffic and offer IPv6 services by December 2011
    - All central and State government ministries and departments, including its PSUs, shall start using IPv6 services by March 2012
- **Indonesia**
  - IPv6 Development Updates in Indonesia Working on Building Awareness of IPv6 - Published by Indonesia IPv6 Task-Force
- **Japan**
  - **Overview Report:** Study Group on Internet's Smooth Transition to IPv6 (Tentative Translation) - Issued by the Ministry of Internal Affairs and Communications (MIC), Japan, June 2008
  - **Report:** Study Group on Internet's Smooth Transition to IPv6 (Tentative Translation) - Issued by the Ministry of Internal Affairs and Communications (MIC), Japan, June 2008

- ▪ **Korea**
  - – [IPv6 Deployment in Korea](#) - by Mr. Park, Syung-Kyoo, National Internet Development Agency of Korea (NIDA), September 2008
- ▪ **Malaysia**
  - – [Moving The Nation TowardsIPv6-Enabled by 2010: Policy and Regulatory Matters](#) - Issued by the Malaysian Communications and Multimedia Commission, Malaysia, November 2007
- ▪ **Singapore**
  - – [Singapore Internet Protocol Version 6 (IPv6) Profile, 2 Jan 2012](#)
  - – **Information Paper:** [Internet Protocol version 6 Phase 2 Transition Plans for Singapore, April 2011](#) - Issued by the Info-Communications Development Authority (iDA), Singapore
  - – [Report for iDA, IPv6 adoption guide for Singapore, 15 March 2011](#) - Published by Analysis Mason and Tech Mahindra
  - – **Information Paper:** [Internet Protocol version 6 Transition Plans for Singapore, June 2006](#) - Issued by the Info-Communications Development Authority (iDA), Singapore
- ▪ **Taiwan**
  - – [Taiwan IPv6 Deployment Current Status](#) - by Sheng-Wei Kuo, Taiwan Network and Information Center (TWNIC), February, 2008

IPv6 provides valuable benefits to agencies by facilitating an improvement in operational efficiencies and citizen services. Many of these benefits will not be fully realized until more complete IPv6 adoption is achieved. 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, when enabled and configured with the appropriate key infrastructure, comes in the form of IPsec, which allows authentication, encryption, and integrity protection at the network layer.
- ▪ **Address Auto-Configuration:** IPv6 address auto-configuration enables simple devices to achieve out of the box plug-and-play network access that is the 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 network address translation (NAT), will allow the optimization of media-streaming applications. This will allow timely video feeds and quality-rich information to be easily distributed to millions of locations.

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

However, in order to realize the benefits offered by IPv6, it is important that the Federal Government continue the process of architecting and deploying secure IPv6-enabled network services.

The adoption of several technology solutions, Classless Inter-Domain Routing (CIDR) addressing, Network Address Translation (NAT), and Port Address Translation (PAT), all helped extend the life-span and availability of IPv4. While some Federal agencies may have enough IPv4 space allocated to support their needs for the foreseeable future, the Internet Assigned Numbers Authority (IANA) address pool was exhausted in January 2011, and several Regional Internet Registries (RIR) exhausted their allocations in April 2011. The remaining RIRs expect exhaustion within the next two years.

Demand levels for addresses continue to accelerate 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 adoption of cloud computing. One of the main advantages of IPv6 is that it re-establishes the P2P connection that was difficult in IPv4 due to Network Address Translation (NAT). IPv6 greatly simplifies the deployment of the Next Generation of the Internet services and technologies, sometimes called the "Internet of Things," providing the "plug and play" experience.

It is important to note that without a concentrated effort by Federal agencies to effectively and efficiently deploy secure IPv6 network services, the U.S. government's technical advancement and ability to meet its mission needs will be critically impacted. The remainder of this document discusses the topics above in greater detail.

> "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
> Former CTO, IPv6 Forum Chair North American
> IPv6 Task Force (NAv6TF)

2. Federal Transition Components

Early initiatives led by the U.S. Department of Defense (DoD) and the Office of Management and Budget (OMB) drove agencies to demonstrate progress in areas of standardization and testing/certification to prepare for eventual government-wide IPv6 integration and transition.

2.1 OMB Guidance

2.1.1 OMB September 2010 Memorandum

On September 28, 2010, the Federal Chief Information Officer issued a Memorandum For Chief Information Officers of Executive Departments and Agencies titled "Transition to IPv6" (http://www.cio.gov/documents/IPv6memofinal.pdf), stating that the Federal Government is committed to the operational deployment and use of Internet Protocol version 6 (IPv6). The memo describes specific steps for agencies to take to expedite the operational deployment and use of IPv6. It went on to explain that the Federal Government must transition to IPv6 in order to:

- Enable the successful deployment and expansion of key Federal Information Technology (IT) modernization initiatives, such as Cloud Computing, Broadband, and SmartGrid, which rely on robust, scalable Internet networks.
- Reduce complexity and increase transparency of Internet services by eliminating the architectural need to rely on Network Address Translation (NAT) technologies.
- Enable ubiquitous security services for end-to-end network communications that will serve as the foundation for securing future Federal IT systems.
- Enable the Internet to continue to operate efficiently through an integrated, well-architected networking platform and to accommodate the future expansion of Internet-based services.

To facilitate timely and effective IPv6 adoption, agencies were asked to:

- Upgrade public/external facing servers and services (e.g. Web, email, DNS, ISP services, etc.) to operationally use native IPv6 by the end of FY 2012.
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014.
- Designate an IPv6 Transition Manager and submit his or her name, title, and contact information to IPv6@omb.eop.gov by October 30, 2010. The IPv6 Transition Manager is to serve as the person responsible for leading the agency's IPv6 transition activities and will liaison with the wider Federal IPv6 effort as necessary.
- Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.

To facilitate the Federal Government's adoption of IPv6, OMB will work with the National Institute of Standards and Technology (NIST) to continue the evolution and implementation of the USGv6 Profile and Testing Program. This Program provides the technical basis for expressing requirements for IPv6 technologies and tests commercial products' support of corresponding capabilities.

"NIST has implemented a tool to estimate the extent and quality of IPv6 (and DNSSEC) deployment in USG, industry and educational networks. Output from this tool can be used to sample agencies progress towards

the 2012 directive goals. This Website is available at: http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov. **Figure 1,** is a partial sample from the website for July 2012.

Transition Managers are advised to check the deployment monitor to verify the accuracy of their list of websites, domains, and mail services that are being monitored.

Figure 1. View of IPv6 Deployment Monitor

2.1.2   Agency Transition Plans

All Federal Government agency leaders were asked to complete an IPv6 Transition Plan, based on a template provided by OMB, by April 2011 to:

- Upgrade public/external facing servers and services (e.g. Web, email, DNS, ISP services, etc.) to operationally use native IPv6 by the end of Fiscal Year 2012.
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of Fiscal Year 2014.

2.1.3   OMB Memorandum M-05-22

OMB Memorandum M-05-22, issued August 2, 2005, laid the groundwork for the early stages of integration by requiring Federal agencies, specifically agency CIOs, to confirm that agencies had successfully demonstrated IPv6 capability over IP backbone networks and reported by June 30, 2008. The memo, broadly circulated among government and industry, specified 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:
http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf.

The Memorandum also directed NIST to develop the technical infrastructure (standards and testing) necessary to support wide-scale adoption of IPv6 in the U.S. government. In response, NIST developed a technical standards profile for USG acquisition of IPv6 hosts, routers and network protection devices. Use of the NIST technical standards and testing for USG Acquisition is codified in the FAR.

2.2   IPv6 Federal Acquisition Regulations (FAR)

DoD, GSA, and NASA published a proposed rule in the Federal Register at 71 FR 50011, August 24, 2006, to amend the FAR to ensure that all new IT acquisitions using Internet Protocol are IPv6 compliant. The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council issued a final rule amending the FAR to require that IPv6-compliant products be included in all new IT acquisitions using Internet Protocol effective December 10, 2009.

2.2.1   Current Applicable FAR Previsions

FAR 7.105(b)(4)

(iii) For information technology acquisitions using Internet Protocol, discuss whether the requirements documents include the Internet Protocol compliance requirements specified in 11.002(g) or a waiver of these requirements has been granted by the agency's Chief Information Officer.

FAR 11.002(g)

(g) Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. The applicability of IPv6 to agency networks, infrastructure, and applications specific to individual acquisitions will be in accordance with standards identified in the agency's Enterprise Architecture (see OMB Memorandum M-05-22 dated August 2, 2005).

FAR 12.202(e)

(e) When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol compliance requirements in accordance with 11.002(g).

FAR 39.101(e)

(e) When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol compliance requirements in accordance with 11.002(g).

2.2.2   Acquisition Guidance

It is detailed in the FAR that agency acquisition processes will be modified to include specification of required IPv6 capabilities as defined by USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program (addressed in section 2.7 of this document). These processes and procedures also need to address procurement of services as well as products.

The acquisition of IPv4/IPv6-based network infrastructure is a collaborative effort between technical and acquisition resources, and between financial and mission management. It is recommended that cross-functional teams be empaneled to develop agency-specific processes and procedures addressing their requirements that can be updated over time, as appropriate. These services specifications are not limited to ISP services. They may also include access methods for provision of application services, including cloud provision.

2.2.2.1 Background

During the late 1980s, the Public Switched Telephone Network migrated from analog to digital technology utilizing a series of technical specifications and protocols labeled Integrated Services Digital Network (ISDN). ISDN included a large number of protocols and equipment configuration options that were not standardized until mid-way through the deployment, which hampered service delivery, product development, rollout, and use for years.

During the initial analysis of the Next Generation Network Protocol, it was determined that IPv6 would not be backwards compatible with IPv4 and this decision spawned a collection of IPv6 protocols that would replace their existing IPv4 counterparts. To avoid the pitfalls experienced with ISDN additional steps need to be taken including standard protocol features and configurations for different classes of devices. Extensive testing of these standard network and device features and functions in multiple scenarios must be completed.

Government and industry experts developed various IPv6 test and interoperability networks, protocol test and certification methods, as well as a minimum set of standard IPv6 protocols and well known options that support IPv6 network operations. The Defense Research and Engineering Network (DREN) was tasked with being the initial USG IPv6 test and evaluation network prior to wider adoption by other parts of the government. Networking experts at NIST had been following IPv6 protocol developments. As part of the initial OMB directive, they developed both standard product profiles and test and certification processes for USG deployment to avoid the past ISDN deployment issues.

2.2.2.2 Equipment Profiles

Three types of network attached devices (sets of functions or capabilities) were defined: routers, end user, and network protection devices. Any device that routes packets, whether it is a router or a server with multiple interfaces that is running a routing application, is considered a router. If the device is not a router but is used to protect the network, servers, or other devices, then it is a network protection device. Everything else is an end user device.

2.2.2.3 Example Case

Organizations with large networks usually develop a standard set of router and switch configurations to deploy across their networks in order to improve service and reduce maintenance costs. As an example, suppose an organization has two sizes of field offices, a regional office, data centers, and headquarters. The smaller field offices have 16/24 port routers with T1 interfaces, while the larger field offices have the same 16/24/32 port routers with fractional T3 (Frac T3) circuits that terminate at the closest regional office. Regional offices connect to at least two of the data centers with OC-3c connections, and headquarters also connects to at least two data centers with multiple OC-3c connections. The data centers are the gateways to the Internet and other networks are interconnected to each other by fractional OC-48(c) connections. If the offices are connected to a service provider network, then the organization's routers and switches would be connected by GigE to the service provider's routers that would terminate these circuits.

This sample organization is looking to replace T1 and fractional T3 point-to-point circuits with service provider based MPLS/VPN "cloud" connections. During the last two tech refresh cycles, all router control and switching hardware was upgraded to the latest firmware supporting version 2.0 of production IPv6 code, memory upgrades were made to higher capacity chips, and all router and switch OS's were

brought up to latest tested, secured production release. This network has a two router vendor policy with mixed devices in the field and one of each at the data centers and headquarters.

As this organization proceeds to add new field offices and enhance backbone interconnectivity, the purchases to support these efforts will need to follow the FAR regulations on IPv6 compliance and support. The organization also builds a project team consisting of Network Engineering and Operations, Server support, IT, and procurement. The team contacts their two well-known router vendors and request any Supplier's Declaration of Conformity (SDOCs) on any existing or new equipment. Network Engineering and Operations personnel dump router configurations, firewall logs and protocol dumps of major links identifying all protocols on the network. Server support identifies all higher layer application protocols. Network Engineering confirms that: (1) their Interior Gateway Router Protocol, the router to router protocol used within the Agencies network, is IS-IS; and (2) the Exterior Gateway Router Protocol, the router to router protocol that is used to advertise the Agencies prefixes to the rest of the Internet, is BGP4.

The network engineering and server support groups have some unresolved questions on IPv6 link layer protocols and their potential interaction with IPv4 in a dual-stacked environment. This is a small agency without the need of a full-time test lab, so through an earlier formal agreement with a sister agency, they run a shared network test lab as they also have some common router configurations. Both service providers who are vying for the MPLS service contract have IPv6 test and integration labs that for a small fee can also be used for IPv6 testing.

The two agencies' procurement groups communicate on issues of common interest. It was discovered that the sister agency has already filled out the IPv6 profile, which was added to the existing standard IPv4 router requirements profile they had been using to purchase for several years.

A wider discussion of the relative responsibilities of procurement and IT offices is given in the USGv6 Buyers Guide at http://www.antd.nist.gov/usgv6/BuyersGuide.html. For a summary of the relevant amendments, refer to http://edocket.access.gpo.gov/2009/pdf/E9-28931.pdf. To review these amendments in their full context, refer to https://www.acquisition.gov/far/index.html.

2.3   Federal IPv6 Task Force
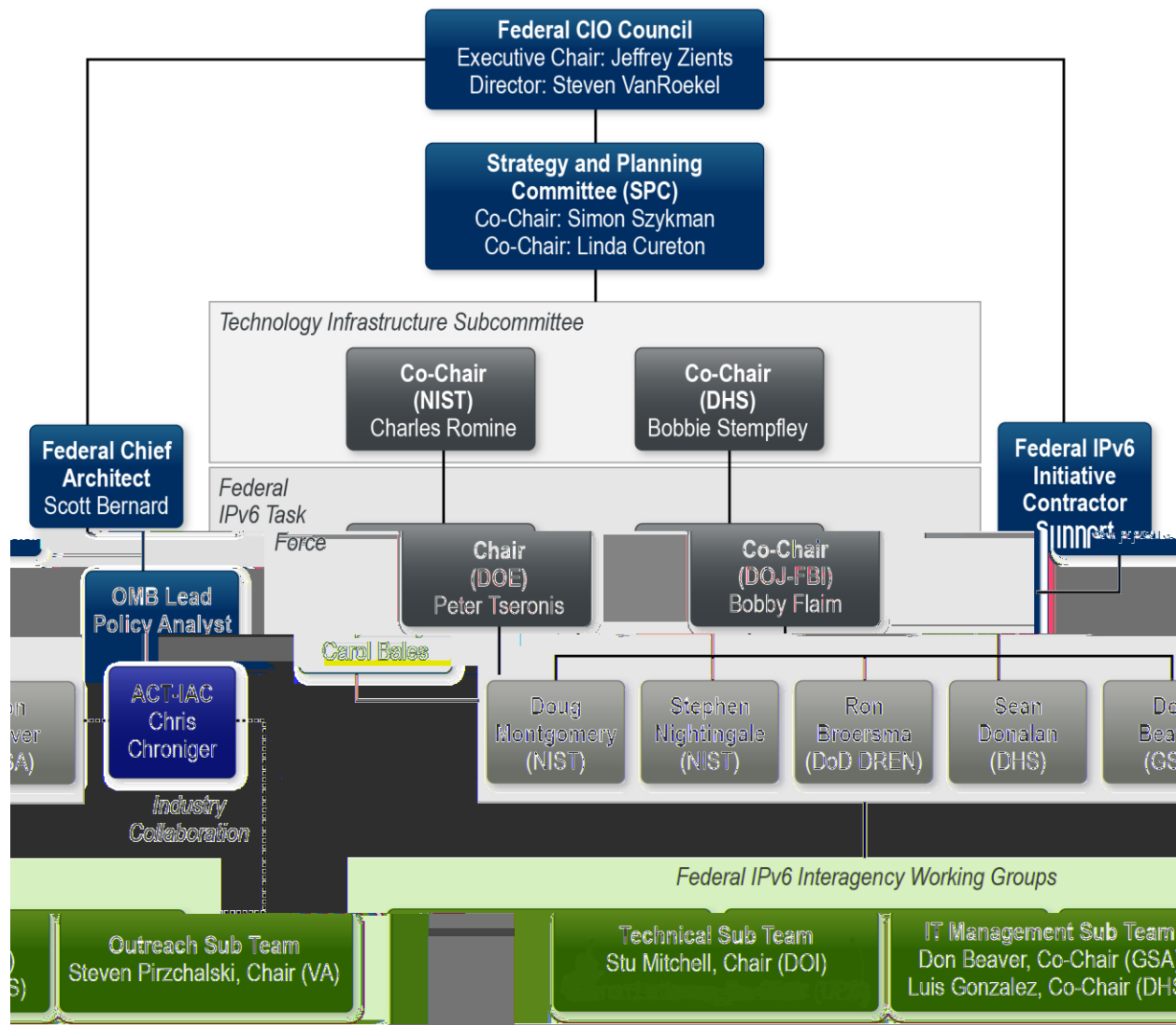
Figure 2. Federal IPv6 Governance Framework

In order to provide better guidance and coordination, the Federal IPv6 Task Force was established to help guide agencies through the IPv6 transition process. Error! Reference source not found., depicts the Federal IPv6 Governance Framework.

2.4   Sample Agency Timelines

2.4.1   Sample Federal Agency Execution Timeline

The IPv6 Outreach Sub-Working Group, described in section 3.6.2, prepared a sample execution timeline for agencies in meeting the OMB-directed IPv6 transition milestones. The first timeline, shown in **Figure 3**, describes the 2012 milestones.

Sample Agency IPv6 Execution Timeline 2012 Public Facing Execution	Key Stakeholders (External)	Milestone 1 06/11	2 12/11	3 06/12	4 12/12	5 06/13	6 12/13	7 06/14	8 12/14
Network Connectivity									
Internet Gateway 1 IPv6 Enabled		Completed							
Internet Gateway 2 IPv6 Enabled	Networx or Other Carriers (ISP)	In Progress	Completed						
Internet Gateway 3 IPv6 Enabled		In Progress	Completed						
Internet Gateway 4 IPv6 Enabled		In Progress	Completed						
Addressing									
ISP Provided IPv6 Addresses	Networx or Other Carriers (ISP) ARIN	Completed							
Announce Agency		In Progress	Completed						
Routing									
Basic IPv6 Routing		Completed							
IPv6 BGP Routing Gateway 1	Networx or Other Carriers (ISP) Routing Vendors	In Progress	Completed						
IPv6 BGP Routing Gateway 2		In Progress	Completed						
IPv6 BGP Routing Gateway 3		In Progress	Completed						
IPv6 BGP Routing Gateway 4		In Progress	Completed						
IPv6 Multi-home Routing			In Progress	Completed					
Domain Name Services (DNS)									
ns1 IPv6 Enabled	GSA (.gov) DNS Providers	Completed							
ns2 IPv6 Enabled		In Progress	Completed						
Ns3 IPv6 Enabled		In Progress	Completed						
ns4 IPv6 Enabled		In Progress	Completed						
Primary Agency Domain (www.agency.com)									
Phase 1	Cloud/Hosting Providers Web Vendors	Completed							
Phase 2		In Progress	Completed						
Mail									
Inbound SMTP IPv6 Enabled	Cloud Hosting Providers	In Progress	Completed						
Outbound SMTP IPv6 Enabled	SMTP/Mail Security Vendors		In Progress	Completed					
Security									
DMZ Basic IPv6 Security	MTIPS/TICAP Providers	Completed							
DMZ Comparable IPv6 Security	SMTP/Mail Security Vendors	In Progress	In Progress	Completed					
Full IPv6 Security			In Progress	In Progress	Completed				
Network Management									
Basic IPv6 Network Management	Network Management Vendors	Completed							
Comparable IPv6 Network Management		In Progress	In Progress	Completed					
Full IPv6 Network Management			In Progress	In Progress	Completed				
Public Facing Domains									
1 Public Facing Domain IPv6 Enabled	Cloud/Hosting Providers Web Vendors	Completed							
35% Public Facing Domains IPv6 Enabled		In Progress	Completed						
100% Public Facing Domains IPv6 Enabled		In Progress	In Progress	Completed					
Pilots									
Mission Pilots	Impacted Vendors/Providers	In Progress	In Progress	Completed					

Legend: In Progress: (green) Completed: (tan)

Figure 3. Timeline for 2012 Milestones

The second timeline, shown in **Figure 4**, describes the 2014 milestones. Note that the 2014 timeline builds upon the 2012 milestones.

Sample Agency IPv6 Execution Timeline 2014 Enterprise Network Execution	Key Stakeholders (External)	Milestone							
		1 06/11	2 12/11	3 06/12	4 12/12	5 06/13	6 12/13	7 06/14	8 12/14
Network Connectivity									
Core/Backbone Network		G	G	T					
Infrastructure Routers 25%	Networx or Other Carriers Routers Vendors			G	T				
Infrastructure Routers 50%				G	G	T			
Infrastructure Routers 100%				G	G	G	T		
Addressing									
Internal IPv6 Addresses Allocated	ARIN DCHPv6 Vendors		G	T					
DHCPv6 Enabled 25%				G	T				
DHCPv6 Enabled 50%					G	T			
DHCPv6 Enabled 100%						G	T		
Routing									
Core/Backbone Network Routing	Networx or Other Carriers Router Vendors		G	T					
Infrastructure Routing 25%				G	T				
Infrastructure Routing 50%					G	T			
Infrastructure Routing 100%						G	T		
Domain Name Services (DNS)									
Internal DNS IPv6 Enables	DNS Vendors		G	T					
Data Centers									
Data Center 1 IPv6 Enabled	Networx or Other Carriers Router Vendors IT Vendors Service Providers	G	G	T					
Data Center 2 IPv6 Enabled				G	T				
Data Center 3 IPv6 Enabled						G	T		
Data Center 4 IPv6 Enabled						G	G		
Mail									
Exchange IPv6 Enabled	Mail Vendors			G	G	T			
Internal Applications and Services									
IPv6 Enabled Apps and Services 25%	Application Vendors Service Providers IT Vendors		G	G	T				
IPv6 Enabled Apps and Services 50%				G	G	T			
IPv6 Enabled Apps and Services 75%					G	G	T		
IPv6 Enabled Apps and Services 100%						G	G	T	
End Device Transition									
Internal Servers IPv6 Enabled 25%	Server and OS Vendors Virtualization Vendors IT Vendors		G	T					
Internal Servers IPv6 Enabled 50%			G	G	T				
Internal Servers IPv6 Enabled 75%			G	G	G	T			
Internal Servers IPv6 Enabled 100%			G	G	G	G	T		
User Computers IPv6 Enabled 25%	Laptop/Desktop and OS Vendors		G	T					
User Computers IPv6 Enabled 50%			G	G	T				
User Computers IPv6 Enabled 75%			G	G	G	T			
User Computers IPv6 Enabled 100%			G	G	G	G	T		
PDA/Mobile Devices IPv6 Enabled 25%	PDA Vendors			G	T				
PDA/Mobile Devices IPv6 Enabled 50%				G	G	T			
PDA/Mobile Devices IPv6 Enabled 75%				G	G	G	T		
PDA/Mobile Devices IPv6 Enabled 100%				G	G	G	G	T	

Sample Agency IPv6 Execution Timeline 2014 Enterprise Network Execution	Key Stakeholders (External)	Milestone							
		1 06/11	2 12/11	3 06/12	4 12/12	5 06/13	6 12/13	7 06/14	8 12/14
Mission Devices IPv6 Enabled 25%	IT Vendors Device Vendors			In Progress	Completed				
Mission Devices IPv6 Enabled 50%				In Progress	In Progress	Completed			
Mission Devices IPv6 Enabled 75%				In Progress	In Progress	In Progress	Completed		
Mission Devices IPv6 Enabled 100%				In Progress	In Progress	In Progress	In Progress	Completed	
Pilots									
Enclave Pilot Phase 1	IT Vendors	In Progress	Completed						
Enclave Pilot Phase 2			In Progress	Completed					
Enclave Pilot Phase 3				In Progress	Completed				

Legend: In Progress: �ध (green) Completed: ▧ (tan)

Figure 4. Timeline for 2014 Milestones

2.4.2   Implementation Recommendations

The Federal IPv6 Taskforce has provided the following guidance to assist agencies with their respective IPv6 planning and implementation:

September 2011

- Aggressively resolved any problems identified
- Integrated Lessons Learned into Transition Plan
- Finalized plan for DNS, review IPsec signing to include AAAA records
- Identified additional public services, including sub agencies
- Planned for mail exchange upgrades
- Publicized successes and build a culture of IPv6
- Acquisition (Agency procurement processes should have IPv6 requirements fully integrated into the acquisition lifecycle and processes.)

December 2011

- Authoritative DNS servers provide transport over IPv6
- Infrastructure components (e.g., ISP, Load balancers, etc.) support IPv6
- Additional sites and services IPv6-enabled
- Completed Support Staff, Operations and Security Staff training and experimentation
- Met with vendors to ensure critical capabilities will be covered

March 2012

- Agencies have a complete understanding of their vendors' readiness and support of IPv6 and have a plan to upgrade/implement/replace components (network, systems, software, etc.) as appropriate and necessary to assure that industry partners are fully capable, compliant and ready to provide implementation of IPv6 configuration within their networks and infrastructure
- Continued progress on enabling public facing services
  – Estimated 10% complete
- Upgraded Operations and Management tools to be IPv6-aware

- Conducted awareness and training for Project Managers, Systems Engineers, Security Engineers, and Change Managers
- Integrated IPv6 requirements into acquisition and COTS upgrade plans. COTS product upgrades applicable to IPv6-capable products only
- Included IPv6 requirements in proposals for all new projects
- Tracked the IPv6 status of all their COTS and GOTS products—Agencies began their platform assessment at this time and are incorporating the results into a spreadsheet or database where all the results are visible in one place. This is a living document/record which reflects all upgrades and changes to products so the sites can track their IPv6 readiness at any point in time. It is important to emphasize that assessments and COTS/GOTS transition plans do not have to wait until the backbone is dual-stack.
- Reviewed agency transition plans— Forward-looking schedules created to bring sites to the IPv6 capability by the target date. This includes proactively upgrading products to IPv6 capability even if there is no tech refresh cycle or engineering change driving the upgrade.

June 2012

- Continued to work with vendor to identify and eliminate IPv6 bugs and workarounds
- Developed a testing and integration process for key fixes
- Continued progress on enabling public facing services (Web, DNS, MX)
  - Estimated 50% complete

September 2012

OMB instructions to the Enterprise Architecture (EA), Capital Planning and Investment Control (CPIC), acquisition and security community to include the following guidance:

- Public facing web services, DNS and email should be 100% IPv6-enabled
- Start integrating milestones to successfully meet 2014 milestones
- Ongoing monitoring will ensure focus is on operational status
- Agencies should have fully integrated IPv6 activities, goals and milestones into the overall governance and management processes to include:
  - **Enterprise Architecture:** IPv6 should be fully integrated into the agencies' Enterprise Architecture including the core design artifacts (e.g., network diagrams and security documentation), as well as the Infrastructure Reference Model and Security Reference Model
  - **Capital Planning:** Agency capital planning processes should include IPv6 in all reviews to ensure that budgets and project plans include the appropriate IPv6 activities
  - **Security:** All agency security processes and reviews should include IPv6

2.5   Agency Progress Tracking

NIST has established a Website to track the progress of agencies in meeting the 2012 OMB milestone for public facing services. The NIST Deployment Monitor can be found at http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov. The Deployment test suite can be found at the USGv6 testing Website via http://www.antd.nist.gov/usgv6/.

2.6   Sub-Working Groups

In transitioning to IPv6 there are a number of common issues that need to be addressed by all agencies with networking best practices. In addition, the IPv6 Task Force believes that despite the complexity and anomalies associated with each agency's networks and infrastructure there is value in sharing best business practices among Federal agencies. To reduce time and effort in resolving these problems and to improve cross agency information exchange, volunteer Sub-Working Groups were established in three general areas: IT Management, Outreach, and Technical.

The leads and members of the IPv6 Interagency Working Group and Sub-groups are interested in learning more about the agencies issues and progress and are willing and ready to assist agencies in learning more about their challenges relative to IPv6 Transition and in helping agencies better plan and transition to meet OMB directives for FY 2012 and 2014.

2.6.1   IT Management Sub-Working Group

The IT Management Sub-Working Group, subordinated to the IPv6 Federal Task Force, is committed to providing support, advocacy and leadership to government agencies and their IPv6 Transition Managers during the transition and implementation of IPv6. The Team is co-led by Mr. Donald Beaver (GSA) and Mr. Luis F. Gonzalez (DHS).

The main goal of the IT Management Sub-Working Group is to assist Transition Managers in successfully assuring the implementation of IPv6 compliance in networks and agency infrastructure per the OMB Federal directive. The Sub-Working group is primarily a conduit of IPv6 information, intervention and support to agencies, providing or facilitating assistance in IPv6 Project Planning, IPv6 Procurement and Acquisition, and IPv6 Vendor Integration.

To this end, the IT Management Sub-Working Group will identify best practices and will share lessons learned from agency experiences and the private sector with IPv6 implementation. The group also envisions its role to collaborate with other Sub-Working groups, as appropriate, to advocate the profound benefits of IPv6 adoption. The sub-working group of the Federal IPv6 Working Group convenes meetings with agency transition managers to better facilitate and accomplish the vision and mission set forth by OMB.

2.6.2   Outreach Sub-Working Group

The Federal IPv6 Task Force identified outreach across government agencies and within industry as a critical aspect of the Federal IPv6 transition. Mr. Steven Pirzchalski (VA) has been designated as the Federal IPv6 Outreach Chair. The goals for the outreach effort include facilitating collaboration and communication between agencies and within industry, sharing information and results and identifying training and other resources to assist in the transition process.

Federal outreach activities include:

- Semi-annual Federal IPv6 conferences
- Direct agency interaction and discussion
- Resource and support identification
- General inter-agency IPv6 training

2.6.3   Technical Sub-Working Group

Another critical aspect of the transition effort is the discussion of technical issues common to the agencies. A Technical Sub-Group co-led by Mr. Stewart Mitchell (DoI) was organized and has a series of monthly roundtable discussions on technical topics of interest to the agencies in cooperation with the ACT-IAC IPv6 Address Planning Sub-group co-lead by Mr. John L. Lee and Mr. Kenneth D. Burroughs.

2.7   NIST USGv6 Activities

2.7.1   USGv6 Profile Process

OMB Memorandum M-05-22 also directed the NIST to develop the technical infrastructure (standards and testing) necessary to support wide-scale adoption of IPv6 in the U.S. government. In response, NIST developed a technical standards profile for USG acquisition of IPv6 hosts and routers, as well as a specification for network protection devices. The Host and Router Profile includes a forward-looking set of Requests for Comments (RFCs), published by the Internet Engineering Task Force (IETF), that encompasses basic IPv6 functionality, and sets specific requirements and key optional capabilities for routing, security, multicasting, mobility, network management, and quality of service.

The Protection Device Profile contains a NIST-established set of capability requirements for IPv6 aware firewalls and intrusion detection systems. 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.

2.7.2   USGv6 Test Program

Following publication of the USG IPv6 Standards Profile, an infrastructure to demonstrate IPv6 product compliance was established. NIST established 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 developed Special Publication (SP) 500-273, USGv6 Test Methods: General Description and Validation, which, taken together with the abstract test specifications published at the USGv6 testing Website, provides the essential material for accreditors to establish testing programs. 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."

Compliance is signaled by device vendors issuing a "Suppliers Declaration of Conformance" (SDOC) 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. This is a critical success factor supporting the FAR direction described in section 2.2 of this document.

The test program is in operation; moreover, accredited laboratories are now in operation and have been testing products with USGv6 capabilities for conformance and interoperability. The latest information can be found via http://www.antd.nist.gov/usgv6/.

2.8   DoD IPv6 Product Profile

A June 2008 Memorandum issued by the DoD Assistant Secretary of Defense – for Networks and Information Integration/DoD Chief Information Officer (ASD NII/DoD CIO) entitled "DoD Internet Protocol Version 6 (IPv6) Definitions," updated the definition of "IPv6 Capable Products" and "IPv6 Capable Networks" in the context of products intended for use in 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 comply with the IPv6 standards contained in the DoD Information Technology (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 6.0, dated July 2011, and is available on the DISRonline at: https://disronline.csd.disa.mil.

The DoD IPv6 Profile provides guidance on applying DoD policy, DISR requirements, 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, as indicated below:

- **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.

DoD no longer supports standalone IPv6 product certification testing. For products identified in the DoD Unified Capabilities Requirements (UCR) document, IPv6 requirements will be validated in conjunction with the larger Interoperability Certification and Information Assurance testing that is conducted on the product for listing on the UC Approved Products List (APL). The detailed IPv6 requirements for UC products and/or functions are provided in section 5.3.5 of the UCR 2008, Change 3 document, and are derived from the DoD IPv6 Profile. The UCR document and the UC APL are available on the following link: http://www.disa.mil/ucco/.

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.

While the documents need not be identical, they must be compatible. Therefore, 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 throughout future updates.

3. The Business Rationale for IPv6

Over the past several years, the robustness, scalability, and limited feature set of IPv4 have been tested by a consistently expanding need for new IP addresses. The surge of new devices and Internet connectivity has continued to accelerate; therefore, the Internet Assigned Numbers Authority (IANA) IPv4 address space is now exhausted.

One of the drivers for establishing the 2012 milestone was the pending exhaustion of IPv4 address space and the realty that soon there would be IPv6-only users on the Internet. This is considered a continuity of operations issue for agencies that provide citizen services or work with external business partners.

With IPv4 address space exhausted, IPv6 is now inevitable as we continue to move toward a ubiquitously connected society. Without the full deployment and support of IPv6, it is just a matter of time before networks become isolated and unable to communicate. The ability to integrate computers with everyday devices, such as mobile phones, handheld devices, tablets, and home entertainment, is no longer a want − it is a need. Without this capability, we will severely limit the move toward a connected society, hindering business efficiency. Federal Government personnel and information workers need integrated, secure functionality that helps them manage their professional lives through the use of e-mail, instant messaging (IM), contact management, shared calendars, and relationship management.

Figure 5 provides a high level business-focused summary of the advantages IPv6 has over IPv4 in terms of features:

Feature	IPv6	IPv4
Easier Management of Networks	IPv6 networks provide auto-configuration 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, demanding increased maintenance efforts.
End-to-end Connective Integrity	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, 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 require IT management.	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.
Unconstrained Address Abundance	3.4×10^{38} = 340 trillion trillion trillion addresses—about 670 quadrillion addresses per square millimeter of the Earth's surface.	4.29×10^{9} = 4.2 billion addresses—far less than even a single IP address per person on the planet.
Platform for Innovation, Collaboration, and Transparency	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; thus, any work on IPv4 has had to find ways around increasing constraints.
Integrated Interoperability and Mobility	IPv6 provides interoperability and mobility capabilities that are already widely embedded in network devices.	Relatively constrained network topologies restrict mobility and interoperability capabilities in the IPv4 Internet.
Improved Security Features	IPsec is built into the IPv6 protocol and is usable with a suitable key infrastructure.	Security is dependent on applications; IPv4 was not designed with security in

Feature	IPv6	IPv4
Capabilities		mind.

Figure 5. IPv6 vs. IPv4 Features

The transition to date has been gradual but the steep curve is starting and it is critical to be prepared. It is also important to note, however, that the transition to IPv6 is more complex than previous advances we have made regarding Internet technology (e.g., from dial-up modems to always-on DSL or from host files to the domain name system). This is all the more reason why the critical step toward the "Next Generation Internet" requires immediate attention and detailed planning to ensure success.

4. Federal IPv6 Transition: The "To Be" State

In 2005, OMB formally initiated the Federal process of transitioning to IPv6 with the release of Memorandum 05-22 which culminated in a successful set of Federal-wide IPv6 tests. In September 2010, the Federal CIO released a new IPv6 directive that established a step-wise approach for agencies transitioning to IPv6. This approach focused Federal agencies on meeting a short-term goal of making their external and public-facing services IPv6 operational by the end of FY2012. A mid-term goal was established to make agency internal services IPv6 operational by the end of FY2014. These goals provide agencies with the operational infrastructure to build truly robust IPv6-enabled end-to-end services in the future that would take advantage of advanced IPv6 capabilities and features.

One of the drivers for establishing the 2012 milestone was the pending exhaustion of IPv4 address space and the reality that soon there would be IPv6-only users on the Internet. This presented a continuity of operations issue for agencies that provided citizen services or worked with external business partners. The expected depletion of IPv4 addresses finally occurred in February of 2011 when the Internet Corporation for Assigned Names and Numbers (ICANN) made the last assignments of IPv4 addresses to the Regional Internet Registries (RIR).

As agencies move forward with their IPv6 transition planning and implementation, the initial strategy focuses on making IPv6 operational in order to meet specific OMB targets or milestones and ensure short/mid-term IPv6 operational ability. Agencies should initially focus on rolling out IPv6 operational capabilities that are overlaid on the existing IPv4 infrastructure and provide comparable features and functionality. This is the most expedient approach and will be the easiest for agencies to adopt to create an operational IPv6 capability in order to successfully reach the 2012 milestone and 2014 milestone targets. However, this approach alone will not provide agencies with the robust IPv6 deployments that will allow them to take advantage of many of the new features and functionality of IPv6.

Agencies also need to develop a deployment approach focused on leveraging the full capabilities and features of IPv6. This could require significant changes in the underlying physical infrastructure, as well as a potentially significant redesign of the enterprise network and of many of the policies and standard operating procedures. Agencies should incorporate IPv6 as part of their technology refresh and make it part of their longer-term IT strategy.

From a longer-term perspective, agencies should evaluate how IPv6 can be rolled into mid- and long-term modernization activities and strategies, ensuring that requirements are being included in existing acquisition and development efforts, particularly for those efforts that will be in operation for extended periods of time.

4.1   The 2012 "To Be" State

The 2012 "To Be" state is focused on ensuring agencies can continue communicating with outside entities utilizing IPv6. With the exhaustion of IPv4 addresses that has occurred and the continuing rapid deployment of broadband services, including those being spurred by the national broadband initiative and the accelerated deployment of mobile 4G and Wi-Fi services, it is clear that IPv6 only users will soon be a reality within the United States. Federal agencies will need to ensure their ability to continually communicate with these users to maintain proper continuity of services and their overall mission. Essentially, all IP-based communications that occur with entities outside of the agency's enterprise network should be available operationally over IPv6.

The following excerpts from the "*Federal Government Adoption of Internet Protocol Version 6 (IPv6) Frequently Asked Questions*" Updated: November 4, 2011 provider better clarification of the services included for the 2012 milestone.

How do you define what is a USG provided "public/externally facing server or service"?

The intent of the FY 2012 requirement is to ensure that any and all networked services that agencies provide to the general public over the Internet are seamlessly accessible via both IPv6 and IPv4. That is, a service that is both accessible external to the agency (i.e., over the Internet) and accessible to general public users.

Internal services (i.e., accessible only within an agency enterprise or intra-net) and external services that are only accessible to sites/users employing virtual private network (VPN) technologies, or to closed user groups (e.g., requiring an out-of-band establishment of a login account) are not in scope of the FY 2012 requirement.

In summary, if there is a USG provided network service that is currently available to all users of the public Internet, that service must be available to a user who only has IPv6 capabilities.

What sites, domains and services are in scope?

Typical examples of public external facing services that are within the scope of the memorandum include external web (HTTP), email (STMP) and domain name system (DNS) services; but the scope extends to any and all such public services provided or contracted by an USG agency. This includes USG network services both named under the .gov top level domain (TLD), and in other TLDs, and includes services that are entirely outsourced to commercial providers.

(Source: Federal Government Adoption of Internet Protocol Version 6 (IPv6) FAQS dated November 4, 2011)

Agencies will need to take an inventory of the services they use to communicate with outside entities. They should utilize multiple methods in ascertaining these services such as active router and switch configuration audits and Quality Assurance tools. It is also recommended that agencies utilize packet capture, protocol analysis and network analyzers tools directly attached to ingress and egress circuits, to ensure they have fully accounted for all services leaving or entering their enterprise. By the end of FY2012, agencies will need to provide IPv6 operational capabilities for services such as:

- E-mail (SMTP)
- Web (including SSL services)
- DNS
- FTP
- Other

In addition to services entering or leaving the agency's enterprise, outsourced services that interact outside the agency should be included in the overall 2012 planning and architecture, such as:

- Cloud Services
- Web
- DNS
- E-mail (may include more than SMTP)

In order for the services to be operational over IPv6, agencies will need to ensure the supporting infrastructure operations are in place and fully functional in IPv4 are also available and functional for IPv6. Examples of these infrastructure services include:

- ISP services

- Addressing and routing
- Security services
- Network management services

The nominal 2012 "To Be" architecture will be focused on deploying IPv6 in dual stack configuration over the existing IPv4 infrastructure. While there may be some difference, the majority of the capabilities, policies, and standard operational procedures will be very similar.

4.2 The 2014 "To Be" State

The 2014 "To Be" state is focused on ensuring the internal segment of the agency's enterprise is IPv6 operational and able to communicate IPv6 traffic from public/external locations. As agencies move toward the 2014 "To Be" state, their plans should focus on ensuring all internal devices, networks, services, and applications that are required for the use of public/external IP-based communications are IPv6 operational. This will impact a significant number of devices, applications and infrastructure on each agency's enterprise network.

The following excerpts from the "*Federal Government Adoption of Internet Protocol Version 6 (IPv6) Frequently Asked Questions*" Updated: November 4, 2011 provided additional clarification of the services included for the 2014 milestone.

How do you define what USG applications "communicate with public Internet servers"?

The intent of the 2014 requirement is to ensure that public IPv6-enabled network services that are provided external to an agency, are accessible to USG users residing in their agency enterprise networks. The definitions of what is meant by "public" are the same. That is, in this case, the same service that an USG client/application is trying to access, is available to everyone on the Internet. The agency clients applications, host operating systems, and supporting networking infrastructure should be IPv6-enabled such that it is possible to establish native IPv6 end-to-end communication between client application and the external IPv6-enabled public server/service.

Typical examples of client applications that access public Internet servers/services include external web (browsers), email (mail user agents), DNS (resolvers), and their host operating systems. Messaging and social media applications that access publicly available network servers are also within scope.

In summary, if there is an IPv6-enabled external network service that is currently available to all users of the public Internet, that service must be available to an Agency network user who only has IPv6 capabilities. Of course, this requirement does not override agency policies that might restrict employee access to such services. But if such a service is permissible to access using IPv4, it must be possible to access the same service using IPv6.

(Source: Federal Government Adoption of Internet Protocol Version 6 (IPv6) FAQS dated November 4, 2011)

As with the 2012 "To Be" state, the nominal approach will be to deploy IPv6 over the existing IP infrastructure. This will limit the near-term deployment value of IPv6, but will allow agencies to achieve an aggressive 2014 deployment date and make IPv6 operational across the enterprise.

In developing the approach to the 2014 "To Be" state, agencies should prioritize their IPv6 deployments across the enterprise to turn up IPv6 in manageable waves as opposed to attempting an all-at-once cutover. Agencies with larger enterprise deployments will find that focusing from a "core out" methodology provides a logical process for transitioning the enterprise that starts with the core WAN/Backbone infrastructure (that should already have been enabled and tested) and then works to sites and finally to LAN segments.

4.3   Beyond the 2014 State

Although the latest memorandum from OMB did not go beyond publicly available services, it is clear that agencies at the very least need to consider mission critical external services that could be impacted as IPv6-only users appear on the Internet. This intent, although not specifically included in the latest memorandum, is not without precedence. In referencing OMB Memorandum 05-22, Attachment C directed agencies to incorporate IPv6 into their specific Enterprise Architectures, including plans for future evolution, and directed the responsible Enterprise Architect organizations to ensure that IPv6 was to be inserted as a technical standard into out year IT strategic objectives. It is now time to ensure that what we put in place for FY2012 and FY2014 is the foundation for the future growth of the Federal Government employment of IPv6.

Examples include telework, citizen services that require login-in or other external business partners that utilize secure communications with agencies. In the next 18 – 24 months as IPv6-only users appear, agencies may lose the ability for telework, or Internet-based healthcare services or a variety of other Internet-based services necessary to meet their agency's core mission, reduce cost, deploy cloud services or improve customer service.

In addition, next steps in the Federal IPv6 transition beyond the 2014 "To-Be" states include 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.

Figure 6 provides high-level examples of IPv6 features and capability enhancements that could be deployed, by Line of Business (LoB), throughout the Federal community:

Line of Business	Objectives/Requirements	IPv6 Feature and Capability Enhancements
Land Use, Mapping, and Agriculture	▪ Resource tracking and allocation via sensor networks ▪ Land boundary and border marking via tags with IP addresses	▪ Ad-hoc routing via neighbor discovery ▪ Address tagging with low-order 64-bit identifiers ▪ Extension headers (location-based services) ▪ Unified Communications ▪ Mobile Applications Access ▪ Teleworking/Distributed Workforce ▪ Sensor Networks
Science, Green Science, and Weather	▪ Improved utilization of existing infrastructure ▪ Sensor networking	▪ Satellite communications ▪ Ad-hoc routing via neighbor discovery ▪ Extension headers (location-based services) ▪ Unified Communications ▪ Mobile Applications Access ▪ Teleworking/Distributed Workforce ▪ Sensor Networks

Line of Business	Objectives/Requirements	IPv6 Feature and Capability Enhancements
Commerce, Banking, and Finance	End-to-end network security authentication and encryption	- IPsec authentication and encryption - Extension headers (financial attributes) - Unified Communications
Information Science and IT Optimization	- Streamlined data flows and reduced networking complexity - Improved end-to-end multimedia and converged - communications - Virtual services and tele-presence	- Flow labels for priority data flows - Optimized hierarchical addressing and routing - Extension headers (variable) - Unified Communications - Teleworking/Distributed Workforce
Justice and Law Enforcement	- Asset deployment identification and tracking - Real-time, ad-hoc, interoperable communications	- Address tagging with low-order 64-bit identifiers - Mobile, ad-hoc routing via neighbor discovery - Unified Communications - Mobile Applications Access - Teleworking/Distributed Workforce - Asset Tracking/ITV
Privacy, Protection, and Security	- Mandatory, end-to-end authentication and encryption - Non-attributable addresses	- IPsec authentication and encryption - Extensive address pool - Unified Communications
Homeland Protection and First Response	- Secure communications - Mobile, ad-hoc communications for first responders - Total force and asset integration	- IPsec authentication and encryption - Mobile, ad-hoc routing via neighbor discovery - Address tagging with low-order 64-bit identifiers - Unified Communications - Mobile Applications Access - Teleworking/Distributed Workforce - Sensor Networks - Transportation Automation (Wireless Access in Vehicle Environments)
Defense, Intelligence, and Military Operations	- Secure, mobile communications - Mobile, ad-hoc communications for warfighters - Asset integration and insightful logistics - Military training/Mission rehearsal	- IPsec authentication and encryption - Mobile, ad-hoc routing via neighbor discovery - Address tagging with low-order 64-bit identifiers - Extension headers (specialize, private use) - Unified Communications - Mobile Applications Access - Teleworking/Distributed Workforce - Asset Tracking/ITV - RFID - Sensor Networks - Transportation Automation (Wireless Access in Vehicle Environments)
Transportation Optimization, Shipping, and Tracking	- Transport and container tracking via sensor networks - Live traffic reporting and communications	- Ad-hoc routing via neighbor discovery - Address tagging with low-order 64-bit identifiers - Unified Communications - Mobile Applications Access - Teleworking/Distributed Workforce - Asset Tracking/ITV - RFID - Sensor Networks
Education, Learning, Knowledge Management, and Library Science	- Improved end-to-end multimedia and converged communications - Virtual services and tele-presence	- Flow labels for priority data flows - Source routing for more efficient transport - Unified Communications - Teleworking/Distributed Workforce - Mobile Applications Access

Line of Business	Objectives/Requirements	IPv6 Feature and Capability Enhancements
Health and Biomedical Science	- Tele-presence - Tele-science (real-time) - Records management and security	- Flow labels for priority data flows - Extension headers (attribution characteristics) - IPsec authentication and encryption - Unified Communications - Mobile Applications Access - Teleworking/Distributed Workforce
Constituent Services (Delivery and Tracking)	- Tracking via sensor networks - Package locations services	- Ad-hoc routing via neighbor discovery - Address tagging with low-order 64-bit identifiers - Extension headers (Location-based services) - Sensor Networks - Asset Tracking/ITV

Figure 6. IPv6 Capability Examples by LoB

5. Leveraging the Common Approach to Federal Enterprise Architecture

As stated in the previous edition to this roadmap, and in accordance with supporting directives throughout the Federal Government, as well as compliance with the Clinger Cohen Act (CCA), the Enterprise Architects are responsible for ensuring the vitality of our respective enterprises by maintaining and enhancing agency architectures in accordance with the IT Strategic Planning process, and supporting the Capitol Planning and Investment Control (CPIC) process for the generation of the Federal Presidential Budget.

The section describes how to use the agency's Enterprise Architecture (EA) and The Common Approach to Federal Enterprise Architecture (CAFEA) as strategic planning and execution tools to enable effective IPv6 deployment. For further details regarding the Common Approach, please refer to: www.cio.gov/documents/Common_Approach_to_Federal_EA.pdf.

There are four primary outcomes enabled by the CAFEA: Service Delivery, Functional Integration, Resource Optimization and Authoritative Reference.

There are eight levels of scope for implementing an architecture using the common approach: international, national, Federal, sector, agency, segment, system and application.

There are eight elements that are part of an agency's EA program: Governance; General Principals which are: Future-Ready, Investment Support, Shared Services, Interoperability Standards, Information Access, Security, Privacy and Technology Adoption; Design and Analysis, Strategic, Business and Technology Principals; Method; Tools; Standards; Use; Reporting and Audit.

Each capability spans six sub-architectural domains in the overall EA: strategy, business, data and information, systems and applications, networks and infrastructure, and security and privacy. These domains are hierarchical (except security which cuts across all sub-domains) in that strategic goals drive business activities, which are the source of requirements for services, data flows, and technology enablement.

The FEAF-II (see **Figure 7**) meets the criteria of comprehensive, integrated and scalable. The geometry of the framework illustrates the hierarchical relationship of the major areas of the architecture, which serves to emphasize that strategic goals drive business services, which in turn provide the requirements for enabling technologies such as IPv6.
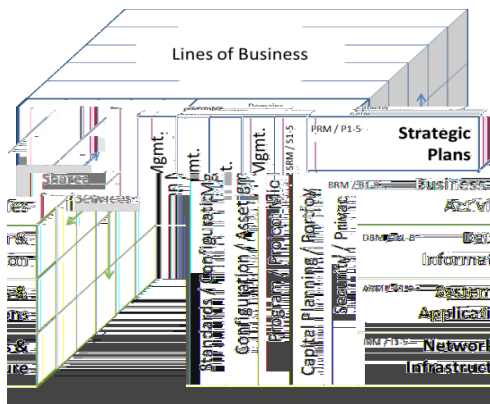

Figure 7. Federal Enterprise Architecture Framework v2 (FEAF-II)

This framework also shows the relationship of sub-architecture domains, how the architecture can be decomposed into segments (that follow structural or functional lines in the organization) and how shared services would be positioned. Finally, FEAF-II correlates the other areas of governance (capital planning, program management, and human capital management); documentation via an enterprise-wide modernization roadmap, a standard set of core / elective artifacts and reporting via standard reference model taxonomies in each sub-architecture domain.

The agency's EA should be used to:

- Assess the "As-Is" IPv4 and IPv6 environments
- Envision your agency's "To-Be" IPv6 state, defining network services to be IPv6-enabled based upon the agency's business needs
- Develop an IPv6 Transition Strategy to address the gaps between the "As-Is" and "To-Be" IPv6 environments
- Identify where to invest in IPv6-enabled network services (as defined in your Target EA) through the CPIC process
- 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 in **Figure 8:**
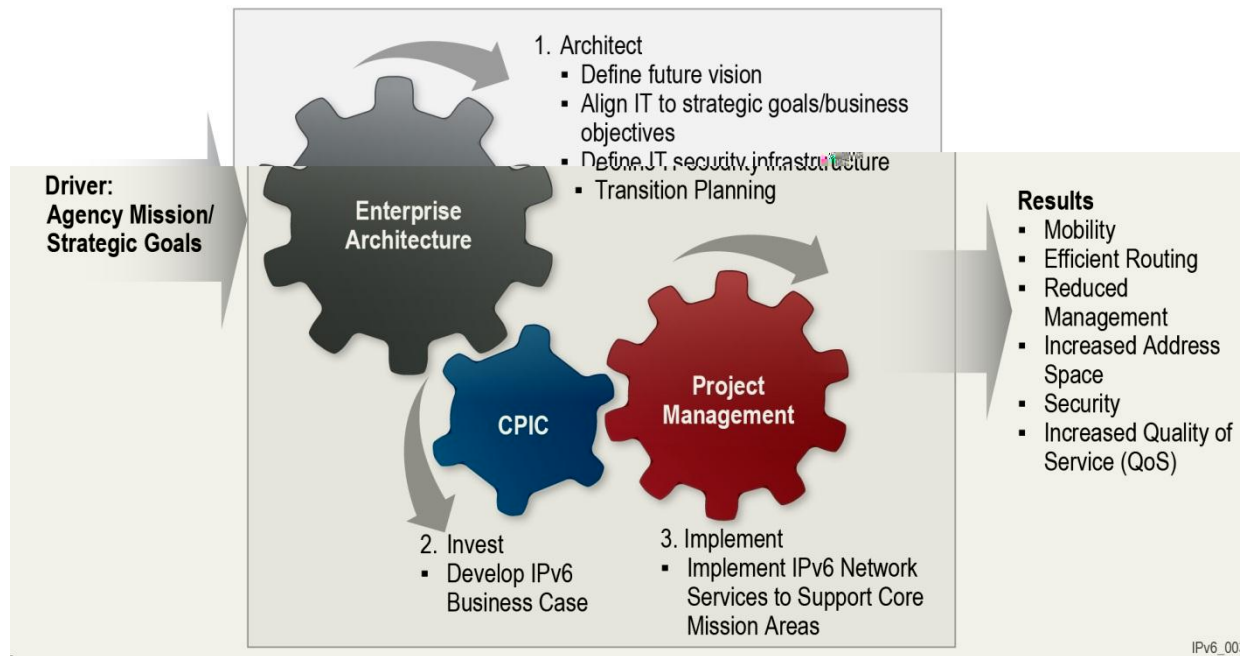

IPv6 Transition Concept of Operations

EA Governance and Management: Governance is the mechanism by which EA planning decisions are realized and enforced within each agency. Agencies should have as part of their EA artifacts governance charters, agendas, and other documentation to demonstrate that:

- The agency body responsible for EA governance is aware of the requirement for IPv6 transition and the specific role IPv6 plays within the agency's target architecture.

- The agency body charged with implementing IPv6 is coordinating its activities with the EA governing body, and changes to either EA or IPv6 implementation policies are effectively communicated to each group.

The EA provides agency managers with the ability to observe the current state of the IPv6 transition within the agency and its impact on other strategic agency initiatives.

5.1 Using the Sub-Architecture Domains

OMB requires agencies to incorporate IPv6 modernization activities into their overall EA as well as the specific Network and Infrastructure sub-architecture domain.

The target architecture should reflect not only the impact on agency networking components, but also the impact of IPv6 on other architectural views such as Business, Strategy, Data and Information, System and Applications; as well as Security and Privacy. Agencies should integrate their IPv6 target visions into the following layers of their domains, as appropriate:

- **Business Activities:** 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 the introduction of telephones and the Internet as examples of infrastructure-enabled business function transformations.

- **System and Applications:** 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
- **Networks and Infrastructure:** 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
- **Security and Privacy:** May be represented as a cross-cutting concern rather than a separate view of the target architecture. IPv6 deployment within the network backbone may have a substantial impact on the target security architecture, including:
  - Changes to network security standards and configuration as a result of the IPv6 end-to-end security model
  - Changes to IT security policy
  - Privacy considerations

Figure 9, 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, as well as the impact that IPv6 has in realizing these benefits.
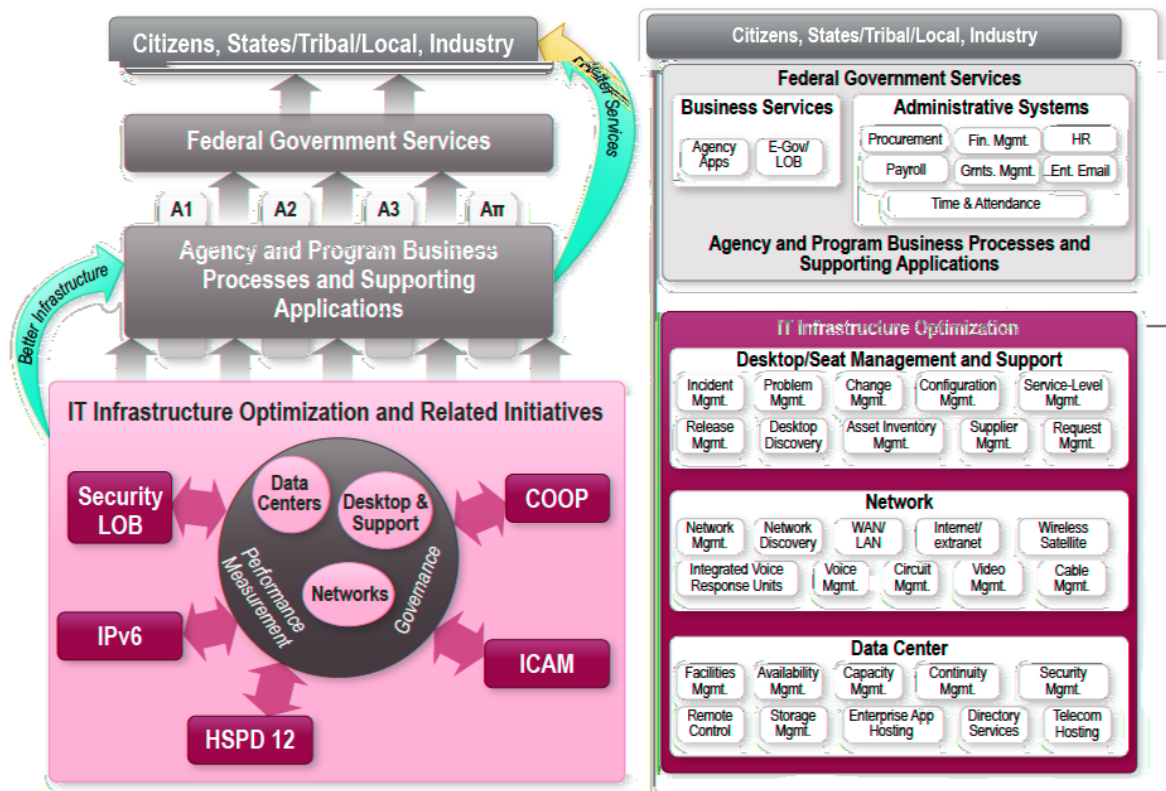

Figure 9. Role of IT Infrastructure Optimization

5.1.1 Developing a Shared Approach to Infrastructure Services

OMB Memorandum 11-29 was issued August 8, 2011 and directed agencies to take a shared service approach to delivering commodity IT, including core infrastructure functions. This approach emphasizes delivering infrastructure capabilities as a "service" to the entire agency rather than as individual components. One can think of this 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 this approach is providing IT Infrastructure services via a pool of resources (Web servers, application servers, database servers, servers, storage instances) instead of through discrete instances. The concept also has a broader usage that includes all configurable infrastructure resources such as computer, storage, and networking hardware and software to support the running of applications.

IPv6 provides significant advantages in the deployment of shared IT infrastructure services, including

- Massive scaling potential
- End-to-end addressing
- Improved network level security
- Auto-configuration
- Mobility

- Modular design with clean extensibility

5.2 EA-Driven IPv6 Planning

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

5.2.1 Define Business Needs and Objectives

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

IPv6-deployment can be:

- **Strategy-driven:** Improving IT Infrastructure quality through security, reliability, agility
- **Core mission-driven**
- **Operationally driven:** Involving a technology refresh or meeting OMB requirements.

> 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).

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

Once a strategic perspective for IPv6 integration is defined at the business level, the next step is to perform a dependency analysis and develop an understanding of the underlying IT services supporting the business strategy. For this effort, it is important to review the application, system, or sub-architecture domain that relates to each IT investment that will be affected 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 below 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/usgv/usgv6-v1.pdf).

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

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: ▪ Premise-based Virtual Private Network (VPN) services ▪ Network-based VPN Services ▪ Audio, video and data communications ▪ Managed notebook/desktop support services ▪ Security services ▪ Application support through the Systems/Data Center services ▪ 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

5.2.3 Identify Each Application's Technology Components, Assessing Changes Required Support IPv6 Transition.

The technology architecture view should be updated to reflect the technology assets that:

▪ Support the potential IPv6-enabled network services

▪ Provide or require IP services and identify whether those assets, such as routers and servers, are capable of being upgraded to support IPv6

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 and dual-stack configurations

▪ Technology hardware and software products

▪ The agency networking topology, if the agency technology architecture extends to this level of detail

5.2.4 Using the USG IPv6 Standards Profile

The U.S. Government IPv6 Standards Profile was developed and released by the 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.

The profile is intended to define a minimal set of IPv6 recommendations to:

▪ Deliver expected functionality

▪ Insure interoperability

▪ Enable secure operation

▪ Protect early investments

The profile is also intended to define a compliance framework to:

- Enable products to be tested against requirement sets
- Document the results of such tests.

Agency standards profiles must align to the standards set forth by the USG IPv6 Standards Profile as shown in **Figure 10**.

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

The recommendations are organized in three ways:

- Into subsets by "device" type (Host, Router, Network Protection Device)
- By functionality (Base, Mobility, Routing, QoS, Transition, Link, Security, Multicast, Application, NPDs)
- By requirement (Unconditional MUSTs, Conditional MUSTs, Optional Capabilities)

Figure 10. Sample USG IPv6 Profile Excerpt

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, provides a quick tabular means of conveying functional requirements and declarations of capabilities between the USG and its suppliers.

The 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 checklist.

5.3 Developing an IPv6 Transition Strategy Plan

Following release of the September 2010 OMB memorandum, agencies were required to complete IPv6 Transition Plans by April 2011. The IPv6 Transition Plan should be folded into the agency's Enterprise Roadmap. It should link to core mission segments, as appropriate, and it should define a specific timeline and set of milestones to deploy secure IPv6-enabled network services defined in the EA and/or Network and 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, be sure to focus on ensuring that network, computing, application, and service components are enabled in a sequence that

> "A change in thinking is required to survive and thrive. Yesterday's thinking won't solve today's problems. Any organization that relies on the Internet to any extent must be prepared to support IPv6. Postponing the inevitable is not wise and will put organization at a competitive disadvantage. When, how and what you do must be aligned with your business goals and overall IT plan. The US Government is showing leadership by embracing, planning and enabling IPv6. Recognizing that pervasive IPv6 based connectivity will enable the next innovative killer app for the 21st century always on communication era."
>
> Yanick Pouffary,
> IPv6 Forum Fellow,
> North American IPv6 Task Force Technology Director

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 an IPv6 Transition Strategy must include are:

- Identification of transition priorities
- Identification of transition activities
- Transition milestones
- Transition criteria for legacy, upgraded, and new capabilities
- Dependencies
- Risks and mitigation strategies
- Maintenance of interoperability and security during transition
- Use of the USGv6 Profile to express IPv6 capability requirements for specific products

- Transition governance:
  - Policy
  - Roles and Responsibilities
  - Management Structure
  - Management Controls
  - Performance Measurement
  - Reporting
  - Management Actions
- Training
- Testing

Please refer to RFC 5211, "An Internet Transition Plan," for additional guidance.

5.4 Integration with Capital Planning

Results-oriented architecture is developed within the context of the **Collaborative Planning Method (CPM)** which is comprised of five phases. 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. Through practice area integration, the Performance Improvement Lifecycle provides the foundation for sound information and IT management practices, end-to-end governance of IT investments, and alignment of IT investments with an agency's strategic goals.

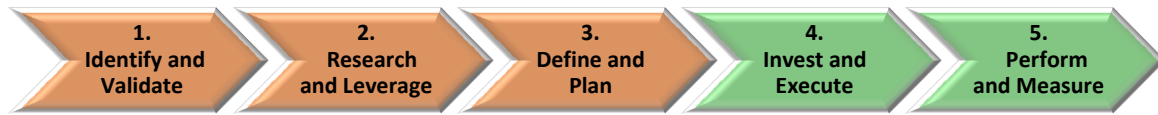| 1. Identify and Validate	2. Research and Leverage	3. Define and Plan	4. Invest and Execute	5. Perform and Measure

Figure 11. FEA Collaborative Planning Method

Error! Reference source not found.**Figure 11,** illustrates the logical integration and sequencing of key architecture, investment and implementation activities in the CPM, as well as feedback from program assessment and performance measurement.

The initial IPv6 Roadmap published in 2009 recommended that agencies develop and submit Exhibit 300 business cases to invest in the IPv6 vision defined by their IT Infrastructure Segment Architecture and Enterprise Roadmap. Moving forward, IPv6 should be a component of all agency business cases that leverage IT capability and services, but not a standalone business case.

5.5   OMB IPv6 EA Assessment Criteria

OMB requires that "the agency's EA (including the Enterprise Roadmap and Network and Infrastructure Sub-Architecture Domain) must incorporate Internet protocol version 6 (IPv6) into the agency's sub-architecture domains and IT investment portfolio. The agency must have concrete plans to deploy IPv6-enabled mission services and applications in its environment.

6. Transition Steps

6.1 Accellerating IPv6 Deployment

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

6.1.1 Develop an IPv6 Test Lab Capability

The total testing strategy discussed in this document includes general purpose IPv6 device testing that is appropriate for all agencies, covered in Section 1.7.2 "USGv6 Test Program." This section provides agency-specific deployment and acceptance testing guidance.

Setting up a testing capability is important for the safe, controlled introduction of new features, technology, and versions of control software into your network and prototyping with an emphasis on validation of targeted behavior and performance outcomes (e.g., experimenting with secure IPv6-enabled teleworking). Testing in a controlled environment 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 to resemble the production environments as closely as possible, including required network services such as DNS and DHCP.

At first, the test sites should not be connected to the production network but be limited to a controlled environment until preliminary testing is complete. During the testing phase, the IT team will gain valuable experience with integrating IPv6, allowing them to determine whether the technology plan or schedule needs to be modified. Once preliminary limited testing is complete, the test environment can be interconnected to other Government IPv6 test networks such as Commerce or the Defense Research Engineering Network (DREN).

It is important to determine what the long-term vision for the dual-stack IPv4 and IPv6 network includes (i.e., the transition approach that will be followed and the tools that will be required to manage the process and the production environment). All technologies, to the extent possible, should be tested in the lab. Ideally, the final test lab configuration will match the production environment as close as possible and may continue to function as an integration lab for future technology refresh requirements.

During IPv6 testing, document successful configurations as well as all interoperability and/or bugs found. The test plan should include IPv4-IPv6 dual-stack capabilities and all network and application services. Induce failure conditions, such as router unavailability, DNS server misconfigurations, 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. Once standard test scenarios have been completed, develop training material and labs and cycle groups of IT staff through to provide hands-on IPv6 training.

After IT staff members have developed solid competence with IPv6, begin production deployment in a few well-defined and controlled locations. During this phase, the pilot site infrastructure should be"IPv6-enabled." At this point, the following steps should occur:

- 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 integrated with the overall agency EA and is configured to handle both IPv4 and IPv6 and set up the DNS and DHCP servers to handle IPv6 queries.

- Configure the associated Network Management Systems (NMSs) to monitor the IPv6 network and infrastructure; as part of the pilot, set up one or more applications that can run over IPv6 so that the agency personnel can expand and build on their existing experience of IPv6 within their environment.

- Continue to test agency specific applications and services, as appropriate, to achieve the 2012 and then 2014 directives.

6.2   Standup Centralized Addressing Authority (CAA)

Due to a lack of routable IPv4 address space, current deployment practices utilize a few globally routable IPv4 addresses that are deployed to front end pockets of RFC1918 or private IPv4 local space. Since the scope of the private address space is very limited, only local control was required. Currently, there are large numbers of overlapping and duplicate RFC1918 space in IPv4 networks that interfere with appropriate network operations, management and cyber security best practices.

Commercial and Government Service providers including Defense Information Systems Agency (DISA) and the Defense Research Engineering Network (DREN) employ a centralized address authority (CAA) as a necessary adjunct to their Network Operations and Security Centers (NOSC) to control and manage their address space. CAA systems can manage existing IPv4 space including overlapping RFC1918 blocks, current or new IPv6 allocations as well as interface to router, switch, firewall, IDS/IPS configuration and management systems.

Current policies also require each agency to request IPv6 space directly from the cognizant IANA addressing authority, a Regional Internet Registry. In North America, this registry is the American Registry of Internet Numbers (ARIN). ARIN policies require:

- Management and control of all blocks and sub-blocks allocated to the organization for periodic review by ARIN or other RIR, especially if additional space is required.

- A single Point of Contact (PoC) per organization requesting and receiving space.

Therefore, it is highly recommended that an agency-wide addressing authority (CAA) be established to:

- Coordinate with the CIO policies, procedures, and requirements for IP based networks.

- Formulate requirements for the management as well as implementation of addressing plans that accommodate network direction for a two to five-year period.

- Develop and maintain an Agency Addressing Plan encompassing both new IPv6, as well as existing IPv4 plans.

- Coordinate address space with ARIN or appropriate RIR, including sub allocation policies within the government agency or organization. (Note: Spoofing of an organization to an RIR has occurred; unfortunately, this can compromise the entire address space and network for that organization.)

> **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.

- ▪ Promulgate allocation policies and procedures and control sub-block allocations to agencies and components within the Department.
- ▪ Coordinate allocations with Service Providers and communities of interest.
- ▪ Stand up an IP address design and engineering tool or capability to help:
  - – Maintain an accurate, current address plan, IP address space plan and operational posture.
  - – Coordinate allocation and delegation of address blocks to:
    - ▪ Agencies and components
    - ▪ Service providers and communities of interest
    - ▪ Operating and support systems (e.g., Provisioning and Configuration),
    - ▪ Network management and network services (e.g., DHCPv6, DNS and ENUM)
    - ▪ Cyber and Network security applications (e.g., Firewalls, IPS/IDS, Deep Packet Inspection)
  - – Meet RIR reporting requirements.

It is also recommended for major agencies or components of a Department to have an addressing authority supporting these subordinate elements. With automated tool supporting CAA capabilities, it is not envisioned that these requirements will require significant additional resources within the agency. A traditional location for this authority would be in the IT organization with management responsibility reporting to the CIO's office.

6.2.1 Address Plan Management and Policies

While address space plans are a major work product of the CAA and some examples of those are located in the Address Plan appendix, the process and procedures framework around them as well as the suite of tools and applications managing and implementing them are a critical foundation for the successful transition and sustainment of next generation Agency networks. The organization and framework for the CAA, as well as the different policies will be agency-specific.

Address Space plans should:

- ▪ 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 should initially follow the existing network topology (i.e., routers and switches and how they are interconnected by communication circuits). As more experience is gained with new IPv6 protocol capabilities, the network topology can be optimized leveraging these new capabilities.
- ▪ Account for evolving government requirements, such as Trusted Internet Connection (TIC), Networx, security, Continuity of Operations (COOP), and geographical diversity.
- ▪ Be maintained in an Agency/Enterprise wide secured database for IPv4 and IPv6 address blocks, subnets and network structures. This current dynamic database serves as the basis for address block and interface status and moves, adds, and changes. Interactive simultaneous access to the data, real time reports and audit information is required for management, security and maintenance activities.

2012 – 2014 Tips: Agencies cannot perform a partial plan for part of the network as it is an integrated whole. Make sure to plan for the network horizon with detailed design and implementation for the 2012 requirements. Routers, switches and other customer facing infrastructure such as servers and network services are required to meet the 2012 requirements. If IPv6 services are not available agency-wide, you

should acquire circuits from IPv6 peering points to concentrations of Web servers or services either logically, physically, or virtually or move the servers to the v6 circuits. This infrastructure needs to be secured from deployment through operational turn up.

Another strategy to meet the 2012 requirements is to use external IPv6 enabled content delivery networks (CDN) for citizen and customer facing service delivery. While the source and validity of this information needs to be maintained, it is for public dissemination and use. If this portal is used for procurement or other sensitive information delivery to the agencies, then additional steps may be required to secure it to appropriate standards.

For example Akamai's[1] CDN / Cloud Services support DNS resolution of AAAA records with both IPv4 and IPv6 transport and dual stacked Web server front ends interconnected to backend Agency IPv4 only content and Web servers. This support is for both http and https traffic. A CDN strategy may not currently support the 2014 objectives of enabling internal agency infrastructure for IPv6 support but supports 2012 requirements for DNS and Web services.

6.2.2   Address Acquisition

Acquiring IPv6 address space is a key step in the transition to IPv6. As previously mentioned, IPv6 space can be obtained from the 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. Agencies can receive space directly from the RIRs and this is Provider-Independent space (PI). For international locations and locations where the routing of PI space is not appropriate Provider Assigned (PA) space can be obtained from an ISP or Service Provider. When obtaining PA space special attention should be paid to peering, routing and transit policies as well as who the peers are for the peering arrangements which need to support the required interconnectivity.

The ARIN Website, https://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. 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 the applying entity's role in requesting the allocation. The primary factor in the RIR request is how much Global Unique Unicast Address Space is required by the Agency for the deployment horizon. The two current default sizes are a /48 for an Enterprise or equivalent, and a /32 for an ISP or larger Enterprise from a single RIR. If your Agency has international sites, then an allocation from ARIN for the North American sites and smaller allocations from Regional ISPs may be preferred, as there may or may not be sufficient requirements for the minimum /48 from other registries. A /32 will be allocated to an ISP, a larger Enterprise or equivalent or an entity acting as a Local Internet Registry (LIR). Setting up a CAA for larger

---

[1] Use of a vendor or product name does not constitute endorsement by the USG and is used for illustrative purposes only.

distributed Agencies allows the CAA to act as an LIR for the Agency and help qualify for the /32 and support RIR reporting requirements.

Current delegation recommendations from a /32 are to assign a /48 to each site. A /48 will give the site 65,535 sub-networks or VLANs which should be sufficient for most locations. If there are mega locations such as large data centers or campuses that would exceed 16 bits of sub-networks, then a larger non-standard block should be allocated to that location. If the 65,535 /48s is not sufficient for the organization then larger blocks can be requested from the RIR following more detailed justification process. If there are a large number of very small sites then a /32 can be requested but for smaller sites, /48s can be allocated.

A table top exercise for an order of magnitude validation could be run on various scenarios with the number and type of locations and different aggregation schemes to validate the size of block being requested. Non-allocated spare blocks should also be part of the calculations as a liberal amount of expansion space should be maintained at all levels of the design. More detail on addressing issues will be available in the Addressing Appendix of this document when it is released in a future update.

The IPv6 addressing architecture also 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 the RFC 1918 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 they should be incorporated in addressing plans.

6.2.3   Establish Address Block Allocation and Management Procedures

Agency wide address management is crucial to assuring unique, consistent and coordinated IPv6 subnet and address assignments across a distributed organization, not to mention accurate provisioning and configuration of associated DNS and DHCP services, equipment network monitoring and management as well as cyber and network security.

To meet network control, management, security and certification requirements an Enterprise Address Management System/Framework (EAMS) is required. An EAMS is a collection of applications/devices that manage IP address and associated information and are integrated together preferably with industry standard open interfaces such as XML. These applications include but are not limited to:

- IP Address Space Plan Management
- IP address block and interface management
- IP address blocks for different routing domains and from different ASNs
- Host DNS resource records (RR), zone identification and DNSSEC control information
- DHCP, DHCPv6 both stateful and stateless, Prefix delegation and other interface address assignment methods
- IP addresses associated with Routers, Switches and other network and end devices configurations

- IP addresses associated with Network and Cyber security devices such as Routers, Switches, Network Access Controllers (NAC), Firewalls, IDS/IPS such as access control list (ACLs), Firewall rules and IDS/IPS signatures.

The IP address management component of the system should support IPv4, IPv6 block management as well as ASN management if required. All major transition mechanisms used by Agencies should be supported, e.g., interface dual stacking, tunnels, by the address management component.

To support dual stacking it is required that the IP address management components support both IPv4 and IPv6 blocks and interface addresses in a single system. It is suggested that existing IPv4 address block and interface assignment data be maintained in the *same system* as will be allocating and assigning IPv6 blocks and interfaces for consistency and coordination. (Note: *same system* does not indicate whether the application / database is on the same hardware, virtual machine, method or mechanism.)

Agencies have different vendors' components which need to be controlled/configured from the EAMS or are a part of the EAMS. Optimally there is multi-vendor compatibility between components in the system for reliability and security.

6.2.4   Interfaces for DHCP, DNS, Network Management and Provisioning Systems

IP address blocks allocated from the IP address management component can be delegated as scopes to different DHCPv4 and DHCPv6 functions across the network. DHCP server functions are implemented in appliances, routers, servers and other devices as well as managed services which for this discussion will not be distinguished but will all be referred to as DHCP servers. It is also assumed for the foreseeable future that DHCP servers will have different instances for IPv4 and IPv6 address assignment and distribution. DHCP servers can also be used to configure other end device parameters if this is permitted by security policy.

The role of DNS has been expanding as Web interfaces are more complex with richer media content and increasing requirements from current laptop, desktop and mobile device operating systems. The number of Resource Records (RRs) in DNS zone files has been increasing to support these new features and functions. The fully qualified domain names (FQDN) for those RRs are getting longer and more complex and the ip6.arpa records for IPv6 are very error-prone if done manually. It is recommended that to the maximum extent possible, DNS RRs be generated automatically from the application doing either the interface assignment or service provisioning. The same system should also generate the ipv6.arpa (reverse mapping of addresses to URI/L) records automatically. The security and authenticity of these RRs should be maintained during generation and transmission to the DNS servers which will then continue the chain of trust with DNSSEC.

Network Management systems require address information from both the Address block and interface assignment and Provisioning function. Network Management Systems maintain the status of all devices attached to the network as well as some device subsystems. NAC functions in switches and discreet systems are employed to exclude rogue non-certified systems from joining the network. Additional exclusion methods include IEEE 802.1x and Link Layer Discovery Protocol (LLDP). Most Agency security policies require network, computing and serving devices to be certified to run on Government production networks as well as routing, switching and other network and security services.

Network provisioning systems are utilized to manage and control router, switch, NAC, firewall and other device configurations necessary for the efficient and secure operation of the network. Router configurations contain Access Control Lists (ACLs) which are used to filter and protect systems from

different types of network and server malware and are used in combination with firewalls, IDS and IPS systems. Best practices require these configurations to be validated in the test network before the configurations are loaded onto Government production networks. If the network has different levels of security or sensitive information, then different Network Management and Provisioning systems may be employed controlling different domains. Some Internet facing servers and system may need isolated Network Management and Provisioning to maintain security domains.

Other end user configuration and provisioning systems are used to maintain standard United States Government Configuration Baseline (USGCB) configurations for end user devices attached to the network. http://usgcb.nist.gov/.

6.2.5   Address Space Plan Management and Address Assignment System

Addressing applications run on a variety of hardware platforms and database systems which include:

- Industry standard appliances, individual and clustered servers
- Virtual Machines either on bare metal or on a host operating system
- Vendor controlled appliances
- Industry standard databases
- Vendor controlled databases

Each Agency's network has different requirements and selection criteria for different network services and the platforms they run on. Agencies are cautioned that unless the networks are small and well contained putting processor and disk intensive network services on VMs is not recommended.

These address management systems concentrate very sensitive network architecture, configuration and openings for malware attacks. These systems should be shielded and firewalled from other systems with secured communications preferably on Government secured industry standard systems. Having a centralized master database that can drive DNS, DHCP, IPAM, NAC, firewalls and other systems that are potential targets of network hackers can avoid the consolidated information being exposed.

Applications are available to design and manage IPv4 and IPv6 blocks to provide a high level to very specific address space plans. Some features (not necessarily available in all systems) include:

- Support for any size IPv4 and IPv6 blocks
- Validate blocks on entry into the system from any source and maintain the accuracy and integrity of the addresses in the system
- Feature parity between IPv4 and IPv6 methods
- Uniquely manage multiple overlapping address space supporting multiple routing domains (the primary example is multiple overlapping RFC1918 space in IPv4 and overlapping IPv6 space between test and production networks and networks in isolated enclaves)
- Generalized tree structure or other mechanism that supports:
  - Delineation of address blocks by network, organization, geographic location, function, etc.
  - Articulate and define address space authority boundaries
  - Visibility and organization of blocks at all levels of the tree
- Commands to manipulate the tree structure including move, add, delete and clone supporting different "what if" design scenarios

- Multiple manual and automated address block allocation, manipulation and reclamation methods maintaining all blocks under management:
  - Manual move and allocate blocks
  - Allocate contiguous blocks or skip blocks to support future needs while maintaining aggregation and CIDR boundaries
  - Allocation of blocks starting at either the high or low block in the range
  - Support pseudo random distribution of a block size across a larger block
  - Automatically breakup larger blocks to fit current allocation size requirements
  - Reclaim a range of blocks and coalesce to the largest available CIDR block
- Generate a DHCPv4 and DHCPv6 scope for DHCP configurations
- Control of blocks by an IP address lifecycle process
- Generalized reporting and interfaces to standard query and report writers
- External interfaces to save and load either partial or complete designs in industry standard formats such as XLS or XML

Address Assignment Features include:

- Support for any size IPv4 or IPv6 subnet either point to point, LAN or VLAN
- Named sub-network blocks for greater accuracy on assigning specific interfaces in large network
- IPv6 specific address types assignments such as /64 EUI-64, /64 Random, and other size IPv6 blocks, as required
- Multiple interface assignment methods such as starting at either the low or high end of a range.
- Audit logs of IP address and user activities
- Equipment which organizes physical and logical interfaces supporting dual stack capability including multiple addresses per physical port
- RIR interfaces to automatically update WHOIS and other records, if allowed
- Manage static and restricted addresses in DHCP configuration
- Generate a DNS RR and .ip6.arpa from an address assignment
- Control of interface assignments by an IP address lifecycle process
- General query and reporting capability
  - Individual addresses, address ranges, equipment and interface connections, amount utilized, which network owns the addresses
  - Which networks the address are associated with
- External interfaces to save and load parts of the network with network structure, address blocks and equipment configuration

Some additional potential system capabilities include:

- Active Directory integration for Personal Identity Verification (PIV) / Common Access Card (CAC) and single user sign on
- User accounts with granular access and control for networks, features and functions including size of blocks
- Multiple simultaneous accesses with granular record locking in the database

- Policy control across the application
- Scheduled and asynchronous events and alerts
- Authorized user access: includes:
  – Standard Agency approved Web browser
  – Java clients to be loaded onto the system and USGCB accredited
- Applications run on industry standard appliances and servers with Web services that allow better performance with much larger number of simultaneous users on clustered servers
- Geographically dispersed high availability servers with Transaction based primary / mirrored database system

6.3 Domain Name Service

DNS systems are an ever increasing component of content rich Web sites, modern browsers and Web applications and are one of the network services required to be IPv6 capable to meet both the 2012 and 2014 directives. For most Government Agencies there are two sets of DNS infrastructure whether physical or logical, one for internal services and users and one for external users accessing externally facing servers and services. DNS systems are sets of DNS servers that start with root or "top level domain" servers such as ".GOV" and eventually resolve to the particular server or service at the Agency they are trying to communicate with.

To meet the 2012 directive customer facing servers, services and infrastructure are being enabled to pass IPv6 traffic accessing these services. In the case of Web servers once the servers and the interconnecting routing, switching and transport service support v6 services, the server IPv6 addresses will need to be populated in customer facing DNS servers. These addresses go into the address field of a "quad A" (AAAA) record to allow the server to resolve the address to terminate the customer traffic. There are several different technologies to support DNS services for the 2012 directive and they include:

- Open sourced, for example BIND, on a Government furnished server or appliance
- A vendor's DNS server software on either an industry standard server or a vendor controlled appliance
- DNS services provided by your ISP, service provider or carrier
- DNS service provided by a DNS services provider or Content Delivery Network

Methods one and two are used for internal DNS services to maintain the more sensitive internal network addresses and topology. Methods three and four are used for external and customer facing services since those are well known publically available addresses anyway. The security issues are prefix hijacking and stealth redirection of customer traffic to bogus sites that are setup for data and keystroke mining of personal information being entered into the "Government systems". Reputations metrics for sites and URLs are becoming are the next valued added services for external DNS services and systems to reduce bogus sites. Existing IPv4 based DNS servers are not touched as a new server or service is brought on line to handle the initial IPv6 traffic. Additionally, at a planned point in the future dual stacked DNS servers are brought online with mixed IPv4 and IPv6 zones.

Specific transition actions include:

- **Requirements:** Develop DNS transition requirements for the organization's 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. RFC 4472 (http://www.ietf.org/rfc/rfc4472.txt) discusses name space fragments, as well as 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.

- **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. In other words, leave the existing IPv4-only DNS servers alone and functioning normally; 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; subsequently, it should be demonstrated as a separate production service.

- **DNSSEC:** 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 well-known cache poisoning bug. The operation of DNSSEC relies on digital signatures to enable data origin authentication and end-to-end data integrity verification. For example an open sourced software 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.

  OMB Memorandum M-08-23 "Securing the Federal Government's Domain Name System Infrastructure" dated August 22, 2008 was Guidance for Implementation of DNSSEC security features in agency (IPv4) networks. The memo indicated that agencies should follow recommendations in NIST Special Publication 800-81 "Secure Domain Name System (DNS) Deployment Guide," and address the particular requirements described in NIST Special Publication 800-53r1 "Recommended Security Controls for Federal Information Systems." NIST Special Publication 800-119 "Guidelines for the Secure Deployment of IPv6" addresses deployment of DNSSEC over IPv6.

- **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.

6.4   Address Assignment Methods

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). 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), which address is assigned, and which additional parameter values are assigned. While providing the most control, it does require proper configuration and administration; however, 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 sub-network 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, which 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, automating subnet assignment and encouraging 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 disabled 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.

If the DHCP server updates DNS, a DHCP server can be configured to sign the update using transaction signatures (TSIG). The 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.

6.5   Network Management

IPv4-based network management systems (NMS) and fault tracing tools must undergo significant change to properly manage IPv6 networks. These would include both equipment and component managers as well as managers of managers (MoM) systems. Service order and network provisioning systems (NPS) are used in the configuration (provisioning), rollout and turn-up of equipment and services in the network. Network management systems, which are integrated with NPSs, then manage the operation and reconfiguration of the systems in the production environment.

These systems can include but are not limited to routers, switches, servers, network services (DNS, DHCPv4/6, IPAM, AAA, and Identity) and various firewalls, IPS/IDS and other cyber security systems. End user devices can also be managed from separate systems which can include validation of end user security software and NAC control. Various quality assurance devices, protocol monitors and other test and evaluation systems are interfaced into the NMS for troubleshoot roles. NMS can also maintain the status and configuration of devices, their IP addresses and other pertinent data and information. System and event correlation as well as x-flow (ifx, J, Net and S) monitors can also be part of the active NMS. NMS can be interconnected to the centralized address repository for initial IP address block and interface assignments as well as system and IP address audits. Utilizing out of band (OOB) encrypted control networks reduces the potential for device control interface compromise and separates less secure data movement circuits from control circuits. For a more complete cyber security posture, the NMS should be interfaced with central address management, network and server security devices. System and device event monitoring and correlation should occur in real time for event detection.

Network Management considerations include:

- No dependencies on IPv4 transport or services but can utilize either transport protocol
- Ability to utilize IPv6 neighbor discovery, ND cache or SNMP MIBs or other methods to perform network mapping if allowed within security policies
- Upgraded for the latest IPv6 and dual-stacked Management Information Bases (MIBs)
- Database and/or storage structures upgraded for IPv6 and dual stack mode
- GUI and documentation upgraded for IPv6 and dual stack.

Some resulting capabilities are but not limited to:

- Full GUI interface for IPv6 features
- Ability to discover and manage IPv6 only and hybrid IPv4/IPv6 devices both network and end node
- Ability to map IPv6 devices and their network structures
- Ability to detect status of IPv6 services such as DHCPv6, IPv6 Routers and switches, IPv6-capable DNS, AAA and other services
- Ability to alert cyber security systems about IPv6 and hybrid devices
- Ability to receive and generate system and device events over IPv6 or dual stacked systems.

Replacing a non-conforming NMS is much more difficult than replacing other hardware or software as it tightly integrates with device software and hardware ports. It is recommended that NMS be upgraded or replaced with IPv6 capable systems prior to the 2014 deadline. Testing of all types and configuration of devices should be completed prior to system cutover and turn-up.

6.6   IPv6 Security

The Federal Government approach to cyber-security may be separated into three distinct elements. Security engineering (employing the government guidelines in designing and deploying secure enterprises; including inserting devices such as firewalls and intrusion detection and prevention systems within the design), security monitoring (employing such processes and devices to monitor for and respond to security breaches), and security certification and accreditation of the enterprise elements in accordance with the Federal Information Security Management Act (FISMA). The Federal adoption of IPv6 impacts all three areas significantly, and merits inclusion within this document. Incorporating at least the three areas stated above into the transition planning work breakdown structure will ensure that the solution generated by the respective agency will be deployed without creating a security breach via either technology or process. The following information is both complementary and supplementary to the NIST SP 800-119 "Guidelines for the Secure Deployment of IPv6". This document must be used as a base reference regarding your IPv6 transition plan regarding security.

While the IPv6 protocol includes many changes, it should be emphasized that many of our existing IPv4 security "policies, best practices and methodologies" are still applicable. A few examples are the use of stateful firewalls, packet filtering, deep packet inspection, defense in depth and the principle of least privilege to accomplish the task. It is not the intent of this

> "Guidelines for the Secure Deployment of IPv6", NIST Special Publication 800-119 is a very thorough treatment of IPv6 protocols and their security by the Computer Science Laboratory of the Information Technology Laboratory at NIST.

section to fully address the entire range of threats and security issues that an operational Government network will be required to face but rather to provide some guiding principles and examples that should help enhance the security posture of the environment and mitigate concerns regarding some IPv6 deployment issues.

While Agencies must evolve their network and cyber security policies, architectures and governance to account for the changing threat landscape and new capabilities within IPv6, they can also leverage some of IPv6's inherent security-related features. Implementing both IPv6 and IPv4 protocols on the same network infrastructure creates two network layers, which inherently increases exposure to attacks. While many IPv4 attack strategies will work in IPv6 such as sniffing, man-in-the-middle, flooding, application layer attacks and rogue devices, new forms of attack are also anticipated. For example, many IPv4-IPv6 coexistence technologies utilize tunneling which requires deeper packet inspection capabilities to scan tunneled packet information than older systems employ. Because production network experience with IPv6 and its resilience to attack is currently limited, proactive steps are necessary to minimize risk. Security monitoring tools, perimeter gateway systems, remediation systems, processes, infrastructure and host security measures need to be tested and qualified in terms of the level of IPv6 protocol support and attack detection/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.

Note that agencies will likely have IPv6 protocols active in their networks, even if they have not specifically deployed them. A strategy of trying to avoid IPv6 and its related issues is not a viable security posture as current operating systems (BSD, Linux, MAC OS X, Microsoft Vista, Windows Server 2008, Win 7 and almost all other "modern" OSs) have IPv6 protocol enabled in their default configurations. Once active, these systems could utilize the default tunneling technology to automatically communicate with the Internet across the agency's network infrastructure without requiring personal intervention. IPv6 capability in these systems should not be disabled at the system level, but unauthorized IPv6 traffic should be filtered at the edge boundaries of the network.

A section on Security, even one strictly dealing with IPv6 issues, is not complete without a brief discussion of the threats against the network, its applications, services, operations and management systems as well as the information processed and stored. Following this section is a list of threats and suggested mitigation strategies based on the different protocol layers. Several of these strategies are general methods that can be used to mitigate multiple threats.

6.6.1   Threats

A number of the most successful threats use simple techniques when attacking organizations that have not yet implemented robust security policies and practices. These attacks can be directed against equipment and services, personnel, contractors and their companies or other business partners. Therefore it is imperative that the entire eco-system implements strong security policies with comprehensive implementation, management and monitoring programs. While a number of these threats occurred on IPv4 networks, hybrid IPv4/IPv6 networks expose a wider opportunity for these threats, requiring updated training/education and enhanced countermeasures.

Statistics in this section were abstracted from the 2011 and 2012 Data Breach Investigations Report[2] (DBIR) which contains a wealth of additional detailed information and should be reviewed by security and networking personnel. Simple data breach attacks usually have a focused purpose of obtaining and extracting information quickly which leaves artifacts on compromised systems both pivot and target, in logs that when found and reviewed by trained personnel can be identified and forensically analyzed. More insidious assaults use stealthy techniques to penetrate and maintain a command and control channel on compromised systems for later exploits.

> Pivot systems are compromised systems within a network enclave which are used to attack other systems on the same network to avoid restrictions such as edge firewall filtering, which may prohibit direct access to the other machines. Targeting control systems in these enclaves belonging to Network Engineering, Operations, Management, Security and Network Services (DNS, DHCP, IPAM and device discovery applications) can be rewarding as users assume access by these systems within the enclave are legitimate.

98% of data breaches in 2011 came from external sources - 6% more than in 2010. The following is a list of methods used:

---

[2] A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit and United States Secret Service.

- 81%   utilize some form of hacking (up 31% from 2010)
- 69%   incorporated malware (up 20%)
- 10%   involved physical attacks (down 19% from 2010, but overall still up)
- 7%   employed social tactics (phishing) (-4%)
- 5%   resulted from privilege misuse (-12%)

An important finding for Government networks and systems is that target selection is based more on opportunity than on choice. Most victims fall prey because they had easily exploitable weaknesses in systems that in hind sight required only simple or intermediate controls to mitigate. What are the common elements to these breaches?

- 96% of the attacks were not highly difficult
- 79% of the victims were targets of opportunity
- 97% of the breaches were avoidable through simple or intermediate controls
- 94% of all of the data involved servers
- 85% of the breaches took weeks or more to discover

These trends indicate that mitigation efforts should be focused on ensuring that essential controls are in place and regularly checked; event and system logs are monitored and mined to proactively identify problems; and the threat landscape evaluated to prioritize mitigation strategies and focus resources appropriately.

6.6.2   IPv6 Capable Network and Security Devices

Several classes of equipment are used to provide a full set of network operations and security functions. Routers (which for this paragraph include switches that route) can be configured to accept and relay route table updates only to and from certain interfaces. Routers, Firewalls, IDSes and IPSes have Access Control Lists (ACLs) that are used to allow or drop different types of packets based on source or destination address, ports, types of service, IPv4 and/or IPv6 traffic and other criteria. Routers and Firewalls can be programmed to drop malformed packets. IDSes, IPSes as well as other DPI or protocol analysis and capture systems have signature databases which are used to scan incoming traffic for malware and other suspicious activity. (Note: a signature is a known series of data or events that have been known to cause harm or indicate malicious intent.) System and event logs from network equipment and services as well as servers can be captured and correlated with other device logs in event correlation systems for real time, periodic or forensic analysis of events to identify precursors and whether actual network attacks are underway.

All of these systems need to have comprehensive IPv6 and IPv4 feature support as well as IPv6 tunneled over/in IPv4 and IPv4 tunneled over/in IPv6 traffic. Management and analysis applications need to be able to monitor application performance across either protocol or a combination of these protocols. Provisioning, network operations and management, configuration management, ACL and signature management systems need to process configuration, ACL and signature files with mixed addresses. These devices should also be capable of communicating over IPv6 to interrogate supported IPv6 MIB structures using SNMPv3.

6.6.3 Address and Configuration Management Systems

In the current dynamic threat environment, manual configuration, maintenance and management of network-relevant information such as IPv4 addresses, IPv6 addresses, ASNs; and of router, switch and security device configurations, are not sufficient. Addresses for network and security infrastructure, servers and end user devices must be tightly coordinated to maintain an adequate, gap free security posture. For more details refer to Section 6.2 "Standup a Central Addressing Authority". During periods of network churn when larger than normal amounts of equipment are being deployed (or decommissioned) on the network, security gaps can be exposed if ACLs on subnets, interfaces and security signatures are not in place when the equipment becomes operational.

Transitioning from an IPv4 to a dual-stack IPv4/IPv6 network has a greater potential as all of the devices in the network should have both types of addresses/connectivity. One of the reasons a phased transition is highly recommended is that it allows for planning, testing, deployment and verification to occur over a well-defined sub-network area.

The network management devices and their control planes should have enhanced protection, as their compromise has a wider impact than individual device compromise.

Addressing plans and device configuration information are extremely productive for forensically tracking vulnerabilities/exploitations of the networks and therefore this information must be well protected with only limited access granted to those with a "need to know". Printouts, presentations, backups and other artifacts of the plans must also be handled as sensitive information. The underlying (or notional) design and structure of the plan may not be as important as most follow well-known network architecture and engineering principals.

It is recommended that complete and partial address plans:

- Be maintained in security enclaves or on systems meeting Agency security requirements and profiles with appropriate physical, logical and network protections in place
- Are stored on systems only to be used for this purpose and have no unessential services or other applications
- Have remote-access only through encrypted VPN IPsec or SSL with PIV/CAC card access
- Not be located in external facing enclaves or network segments
- Allow performance requirements and security policies to dictate whether these should be on physical or virtual servers. This analysis should be based on real-world network characteristics of the environment and not solely on general guidelines but also based on major network events requirements and not just normal operating conditions.

Storing these plans and related addresses in a number of systems or appliances distributed around the network should be discouraged since security requirements increase with the number of devices.

6.6.3.1 Network Engineers, Operations and Management Control Systems

As networks and management systems are hardened, bad actors move up the system/network hierarchy to the computers that control these other systems.

It is recommended that the Principle of Least Privilege (PoLP) be implemented/followed for management systems. Additionally:

- Separate computers are used for address plans, network operations and management, as well as security operations and management and these systems are never connected to the Internet. Security policies that allow using encrypted VPNs to transit the Internet are not addressed here.

- Personnel should have separate systems for official e-mail and authorized surfing of Internet resources as well as appropriate procedures for migrating data and required files to the enclaved management systems. Non-official e-mail and general Internet surfing should not be allowed on these systems as those are primary threat vectors.

- Management of network services and systems should occur over standard communication protocols which can be secured or filtered by firewalls, IDS and IPS systems, additionally comprehensive event logs should be maintained centrally/securely.

- Networks should be segregated into separate management areas, especially Internet facing enclaves, so that in the event of compromise of one management system the entire network will not be compromised.

6.6.4 Defense in Depth

Defense in Depth (DID) is a standard military strategy as well as a network security technique for limiting successful penetrations of IPv4 and IPv6 networks. The DBIR report noted a marked increase, over the last two years, in unauthorized physical penetrations of targets for reconnaissance and data theft purposes. This suggests that rogue systems with malware and spy software can be at any "physical" location in the network, even inside of security perimeters. It is recommended that Network, perimeter, and host based firewalls as well as detection and mitigation strategies be deployed throughout the network to increase the likelihood of stopping or preventing individual or coordinated attacks. Large networks should be architected with intermediate security perimeters to limit access to sensitive information and systems, once outer defenses have been breached. Rural and shared tenant facilities, for example, may need to be firewalled from more sensitive core networks since they may have less secure physical access controls.

6.6.5 Reconnaissance

Reconnaissance (recon) including device, network topology and service discovery is the first and most-basic step for both external and internal compromise. Recon is the enumeration, identification and mapping of network topology, devices, hosts, services and security infrastructure. As Recon has both a legitimate and nefarious purpose, security systems need to alert on any detected Recon activity and maintain sufficient logs to further analyze the intent.

Reconnaissance is normally a precursor to an impending or future attack against the network, its devices, protocols and services including network management, DNS and security infrastructure.

6.6.5.1 Device and Network Topology Discovery

Early in the implementation of IP protocols *ping* and then *traceroute* were developed to troubleshoot networking issues. A class of applications have since been developed to identify devices, what addresses and interfaces they are attached to, fingerprint the type of device and trace through, and if possible to trace through routers and switches to ascertain network topology. Base IPv4 protocols as well as non-standard protocols have been used or piggybacked on to bypass firewalls, IDSes and IPSes to extract the data to collection systems. The network management justifications have included:

- Identify network and end user devices that are not known to network operations and security management
- Identify "Rogue" or unauthorized devices that have been attached to the network
- Use as a simple device and network management technique

A more proactive method would be to impede the attachment of the device / use of the service at all, versus waiting until it has connected and been collecting information. Device and network topology discovery applications are not authorized or allowed on service provider, sensitive and secured networks. It is recommended that these applications not be permanently attached to operational networks as they generate redundant data and can be exploited. Some of the operational issues and mitigations are:

- Out of Band (OOBA) networks are utilized to manage all network gear. This may be either a physically separate management network or a logically separate network. Regardless, for security devices a physically distinct / separate / disconnected network is highly recommended to segregate security operations from network operations and management.

- Router and firewall ACLs should filter / drop several types of ICMP packets on data interfaces only allowing pinging on loopbacks from management networks. Certain types of ICMP packets are filtered from external and internal router and firewall interfaces. (Note: that some types of ICMP messages are critical to the proper operation of IPv6, and must not be blocked.)

- Network Access Control (NAC) and Network Admission Control (NADM) are used to prohibit unknown or un-certified devices on network segments. Switch and router port controls are also employed. This does not prevent physical tapping of copper of fiber connections, which is why physical access controls are still important.

- All network devices on operational networks should be managed by a network operations and management system which will already contain the status of devices and the IP addresses they are attached to. These systems are also used to manage equipment configurations including routing configurations, ACLs and signature databases.

6.6.5.2   Encoding Information in the Interface ID

With the increase in the size of the IPv6 address space, it was recognized that manual IP address management methods would have to be replaced by automated systems. The associated increase in the size of the host ID to 64 bits, led to the practice of encoding network information, usually legacy network information, in the host ID field needlessly exposing the sensitive information. Use of a secure IPAM system to maintain this dynamic information is more scalable, secure and less of an operational load when addresses change.

The large Interface ID field within each IPv6 address makes traditional, brute force network layer address scans extremely difficult, though not entirely impossible, assuming 64 bit subnet identifier and good IPv6 address selection techniques.

Encoding network information and structure in the interface ID portion of the address can aid the intruder in network reconnaissance. From the security perspective encoding of VLAN identifiers, service types, location, types of equipment or service supported should be maintained in the address and network topology management systems and protected from unauthorized access and disclosure. Some examples of these encodings are:

- In a VLAN environment, VLAN ID may be assigned to a portion of the IPv6 Interface Identifier (IID), making it easier to identify the source or destination of the VLAN traffic.

- Decimal or hexadecimal encoding of IPv4 address within the Host ID portion of an IPv6 address. (Deprecated in RFC 4291)

- Encoding service types in the Host ID (RFC 5375), such as HTTP (80), DNS (53), SMTP (25) as a method to identify the services available on the device

- Creating the Host ID partition of an IPv6 address to reflect the location, group and user of the end node

(Note: the normal justification for encoding this type of information in the Host ID is from a management and operations perspective which is based on spread sheets and deprecated IPv4 concepts.)

6.6.5.3   Recon Mitigation Techniques

Techniques employed to reduce recon effectiveness are also used to mitigate layer 2 and 3 threats. Some of these techniques are:

- Consider implementation of privacy extensions for Interface IDs, especially for laptops and mobile devices. Be sure to factor in how this may complicate your forensic analysis and plan to mitigate accordingly.

- Filter internal-use (e.g. unique local) IPv6 addresses at border devices

- Disable unnecessary layer 2 and 3 services

- If services are required in one part of the network but not others, filter those unneeded services at the boundary firewalls or edge routers

- Selectively filter Internet Control Message Protocol (ICMP), largely in accordance with RFC4890

- If providing multicast routing services, ensure proper boundaries are defined and filter at those points appropriately (e.g. by site, organization scope)

- Maintain host and application security in accordance with current best practices and guidance, including routine patch, regression and penetration testing cycles

- Ensure host-based firewalls are IPv6 capable and have appropriate IPv6 rules in addition to the current IPv4 rules

- Secure network engineering, operations, management and services devices such as DNS, DHCPv6, IPAM, xFlow monitoring, servers and log files, server logs, NMSs

6.6.6   Layer Two Threats

The standard sub-network mask size in IPv6 is a /64 which allows an extremely large number of devices on the local link. IPv4 link layer protocols were developed to work with a maximum of 254 devices on a local link, therefore a new link layer protocol was developed for IPv6 based on Internet Control Message Protocol version 4 (ICMPv4), ICMPv6. (Note: ICMP is the control channel for IP networks.) ICMPv6 supports the ICMPv4 features of router redirects, destination unreachable, echo request and reply (ping), packet to large and packet exceeded hop limit. Neighbor Discovery (ND) messages were added to ICMPv6 which include determination of link layer addresses for neighbors on the same local link, address auto configuration, duplicate address detection (DAD) and local router detection. Since IPv6 uses ICMPv6 for ND link layer broadcast messages are no longer needed. ND is used in network addressing to provide address resolution and address auto configuration utilizing Neighbor Advertisements (NA), Neighbor Solicitations (NS). ND is also used for on-link router discovery utilizing

Router Advertisements (RA) and Router Solicitations (RS). RAs provide network prefix information, default route to nodes and can tell the node to use SLAAC and/or DHCPv6 for both IP address assignment as well as configuration parameters. The same types of IPv4 threats have their equivalent IPv6 threat.

Some of these threats are:

- Spoofed RAs can be used to renumber hosts on the segment or launch a Man in the Middle (MITM) attack and siphon LAN traffic for capture
- Forged NA/NS messages to confuse NDP
- ICMPv6 Redirects which are the same as IPv4 redirects
- Forcing nodes to believe all addresses are on-link i.e. denial of service (DOS) attack

These attacks require the computer to be attached wired or wirelessly to the LAN.

Compromised hosts can be programmed to send false RAs on the local LAN segment to redirect all traffic through that host. This allows external agents to inspect, capture, encapsulate and forward sensitive traffic to external IP addresses. Some methods of preventing rogue RA sources include:

- Prevent unauthorized LAN access
- Disable unused switch ports
- Implement NAC, NADM, IEEE 802.1x port based access control, IEEE 802.1AE Media Access Control (MAC) security
- RA Guard (RFC 6105)
- Port based security (pACL)
- Implement Secure Neighbor Discovery (SEND)

The hacker community, specifically The Hacker's Choice (THC) has developed methods to thwart RA Guard and these include:

- NDP messages should not contain extension headers
- Techniques involving fragmentation to avoid detection
- Adding extension headers to RA messages to confuse security tools that do not parse the entire RA message

6.6.6.1 Dynamic Host Configuration Protocol (DHCPv6) Attacks

These techniques involve providing false information during the address negotiation process with DHCPv6 servers.

Mitigations include:

- IEEE 802.1x port based access control and authentication
- Filter DHCP solicits by a "known list" of device unique IDs (DUIDs)
- Monitor DHCP server logs for failed address allocations

6.6.6.2 Link layer Broadcast Amplification Attacks (Smurf):

This is a Denial of Service (DoS) attack where other link layer nodes are tricked into flooding packets to a single node on the subnet.

This type of attack was demonstrated in early IPv6 stacks, but has diminished as more robust implementations become available. Properly implemented IPv6 stacks will not be susceptible to this attack, however this should still be part of IPv6 stack testing.

6.6.7   Layer Three Threats

As in layer two threats a number of layer three threats follow the same pattern as their IPv4 counterparts. To improve packet processing speed, variable length IPv4 packet headers have been replaced by fixed length IPv6 packet headers with Extension Headers (EH). The concept of EH was introduced to provide similar and sometimes enhanced functionality in the IPv6 protocol. The base header is the first part of the packet received and analyzed. Additional extension headers, if used, occur after the base header and several extension headers are chained together and occur before the packet payload. The entire packet must fit in the Maximum Transmission Unit (MTU) of the path of the network routing and switching equipment. In IPv4 when the packets were too big to transit a link there would be local fragmentation of the packet as it entered the link and re-assembled at the other side. In the IPv6 protocol the host, not the intermediary device, is responsible for ensuring delivery through the fragmentation of packets. This fragmentation can cause problems with security devices detecting and protecting against attacks.

Also ensure network and application layer vulnerability assessment tools have the ability to perform security testing with and without fragmentation, across IPv4, IPv6 and dual stack.

6.6.7.1   Network Addressing

Stateless Address Auto Configuration uses the interface port's MAC address to construct the Interface ID in an IEEE standard. The MAC address can be used to determine the manufacture and model of the interface card which can imply the type of computer and operating system. These addresses should not be exposed to the Internet or other non-secure environments.

Address assignment to hosts and routers, unless the host is publicly resolvable in DNS, should use non-obvious, non-guessable addresses. Stateful address assignment should be random and not sequential.

6.6.7.2   Packet Header Manipulation and Fragmentation

IP header modification and crafted packets are used to evade security devices and to attack network infrastructure. IP header and packet modifications include forging source addresses, incorrect sequence or a large number of nested extension headers. There are rules for extension headers that include Hop-by-Hop and destination options. Crafted packets with large chains of extension headers, separation of payload into second fragment and invalid extension headers can consume resources in a DoS attack. Some mitigation techniques include:

- Deny IPv6 fragments on intermediate routing devices
- Block Any and all "overlapping fragments" in accordance with RFC5722
- Block all routing headers type 0, source routing and configure hosts to not act on it
- Apply filtering rules if IPv4-IPv6 translation technologies in use
- Monitor router and firewall counters for fragmentation and header manipulation events

6.6.7.3   Layer 3 and Layer 4 Spoofing

Crafted packets (spoofing) allow attackers to appear to be coming from a different location and/or for another application. Some prudent actions are:

- Filter.IPv6 BOGON (Martians) which include:
  – Filter traffic from unallocated space and filter router advertisements of bogus prefixes
  – Permit legitimate global unicast addresses
  – Do not block FF00::/8 or FE80;;/10 as these will block NDP
- As of this publication date the IPv6 full bogons list is over 32,000 prefixes
- Advertise only your own address blocks
- Hierarchical addressing and ingress/egress filtering can catch packets with forged source addresses
- Use inbound infrastructure ACLs (iACLs) that deny packets sent to infrastructure IPv6 addresses
- Implementation of source address validation of packets may prove to be easier in IPv6.
- Implement DNSSec to authenticate servers

6.6.7.4   IPv6 Firewall Policies

Do not simply use your IPv4 policy for IPv6, instead start with a separate policy and let it grow as your deployment grows. Do not automatically allow IPsec or IPv4 protocol 41 through the firewall. (Note: some hosts may have multiple IPv6 addresses so this could complicate firewall troubleshooting. Deny packets for transition techniques not used.

6.6.7.5   IPv6 Intrusion Prevention

Currently few IPS signatures exist for packets with tunneled protocols such as 6in4, 6to4, 6in6, ISATAP, Teredo, 6rd and DS-Lite. IPSs should send out notifications when non-conforming IPv6 packets are observed having faulty parameters, bad extension headers or the source address is a multicast address.

6.6.7.6   DNS Implementations

Implement DNS in a 'split horizon' configuration, separating internal naming from the Internet naming. For your Internet and customer facing DNS servers, evaluate outsourcing the service as opposed to an Internet facing secure enclave with all of the network operations, management and security issues involved. Additional items include:

- Only expose global devices addresses assigned to internal devices when authorized
- Monitor for DNS enumeration as an early indicator of an attack

6.6.7.7   Routing Attacks

Routing attacks are used to intercept and divert packet traffic, disrupt network routing and make unauthorized modifications to the routing tables. Mitigation techniques include:

- Use existing authentication mechanisms for BGP, IS-IS and EIGRP when deployed
- Use IPsec with OSPFv3 and RIPng
- Use "Passive Interface" on user-facing segments to prevent hosts from participating in the routing protocol
- Filter routing protocols on non-peering external links

6.6.8   Above Layer Four Threats

6.6.8.1   Viruses, Worms and Social Engineering

Attacks at other layers of the protocol stack are unaffected by the security of IPv6. Buffer overflows, cross-site scripting, SQL injection and   E-mail, SPAM, phishing and social engineering attacks are protocol agnostic. These attacks will need to be mitigated with appropriate programming, security policies, procedures and training.

Viruses and worms that rely on current IPv4 network scanning techniques will be limited in their attack and replication capabilities due to the size of the IPv6 address space. However, malware that relies on DNS scraping, local device address information or emailing victims will be unimpeded by the size of address space.

6.6.8.2   Government and Contractor Developed Applications

Internally developed applications which communicate across the current IPv4 network, will need to be tested to ensure vulnerabilities are not created once the application is installed in a dual stack environment.

7. IPv6 Impact on Federal Initiatives

The USG has numerous Federal-wide initiatives underway to improve the overall security and operability of the Federal-wide Enterprise Architecture while limiting or reducing cost. **Figure 12**, depicts a number of initiatives that may appear to be separate but are intrinsically linked. Many agencies are tackling these initiatives in a silo fashion and do not fully understand how each is related and will ultimately impact new "to be" architectures being developed.
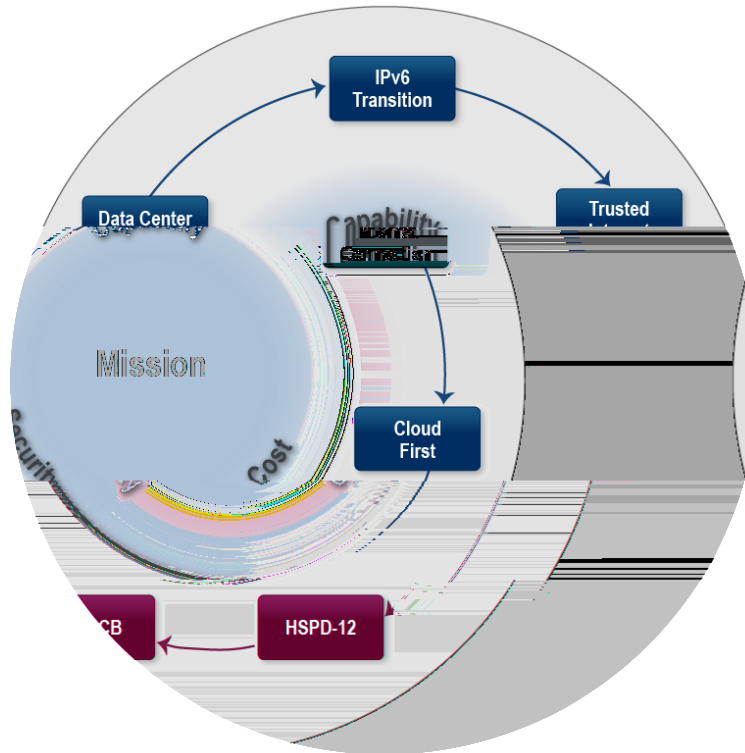

Figure 12. IPv6 Relation to Other Federal Initiatives

This section examines the potential IPv6-related impacts that 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 develop solutions sets that may potentially be conflicting or counterproductive.

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

7.1   Trusted Internet Connection

The overall purpose of the Trusted Internet Connections (TIC) Initiative, as outlined in OMB Memorandum M-08-05, is to standardize and optimize the security of individual external network connections, to include connections to the Internet, currently in use by the Federal Government.

Ultimately, the initiative will improve the Federal Government's security posture and incident response capability through the reduction and consolidation of external connections, and it will provide enhanced monitoring and situational awareness of external network connections by TIC Access Providers (TICAP). A TICAP is the entity responsible for managing a TIC, which is the physical location an agency utilizes to meet the objective of the TIC Initiative.

7.1.1 TIC Objectives

- Reduce and consolidate external connections through TIC Access Providers (TICAPS)
- Develop and maintain baseline technical requirements for TICAP Network and Security Operation Centers (NOC/SOC)
- Oversee Federal agency transition to approved TICAPs
- Maintain relationships with agencies and stay informed with their concerns, including TIC Compliance Validations (TCVs)

Federal agencies also have an option of leveraging an outsourced Managed Trusted Internet Protocol Service (MTIPS) that can be acquired via the GSA Networx contract. GSA has authorized the following vendors to provide the MTIPS service:

- AT&T
- CenturyLink (Qwest)
- Sprint
- Verizon

MTIPS provides security for agencies' online traffic and delivers many other cyber security solutions. GSA and DHS jointly developed the requirements for this Networx TICAP service. (Note: GSA Office of Network Services is currently planning for an MPTIPS 2.0 Acquisition in the summer of 2012.) The high-level functional components include:

- Internet access
- Hosted EINSTEIN enclave (a computer network intrusion detection system)
- Security Operations Center (SOC)
- DCID 6/9-compliant Sensitive Compartmented Information Facility (SCIF)
- MTIPS transport

All information exchanged with the external networks is monitored by the MTIPS Security Operations Center to protect agency traffic, as depicted in **Figure 13.** The MTIPS transport serves as a collection network for the TIC portal, insulating an agency's internal network from the Internet and other external networks.

As of this writing, agencies should have determined their path forward by selecting one of the following options:

- Becoming a TICAP provider
- Acquiring TIC services from another TICAP provider (another Federal agency)
- Acquiring TIC services from a MTIPS provider (AT&T, Qwest, Sprint, Verizon)
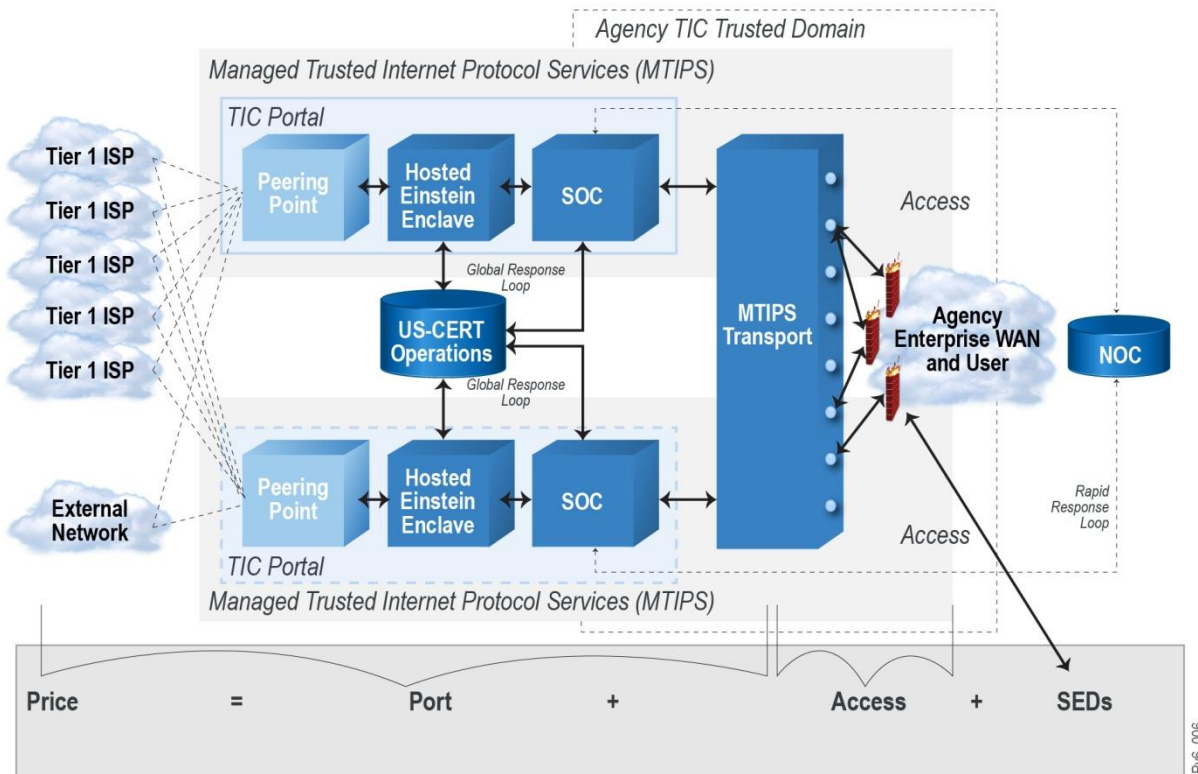
Figure 13. TIC Architecture

Regardless of the option selected, agencies should integrate the IPv6 project with the implementation of TIC, ensuring that the integrated design provides the services and capabilities required to achieve both the TIC and IPv6 goals and objectives. IPv6 considerations for 2012 include:

- IPv6 firewall functionality
- IPv6 IDS capability
- IPv6 DNS
- IPv6 tunneling
- IPv6/IPv4 translation

For 2014 additional elements include:

- IPv6 address and network management
- IPv6 policy

For outer years as IPv6 becomes more prevalent:

- IPv6 routing/traffic
- Support for IPv6 based IPsec
- IPv6 privacy/address hiding

Throughout this Planning Guide/Roadmap to IPv6 adoption, specific design and implementation recommendations have been made that should be integrated into the design and implementation of the TIC program. Agencies should conduct IPv6 readiness reviews of their TICs by obtaining SDOCs, conducting a gap analysis, and implementing upgrade plans.

7.2   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 independently 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 are required to have HSPD-12 Personal Identity Verification (PIV) 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 and cloud computing 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 reducing extensive capital infrastructure investments.

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

7.3   IT Modernization

OMB Memorandum 11-29 (August 2011) directs agency CIOs to consolidate duplicative IT infrastructure networks and services. As agency IT modernization efforts move forward, IPv6 will have a major impact on many infrastructure-related initiatives. Agencies should coordinate and include their IPv6 transition activities within the scope of IT modernization. In particular, 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 USGv6 profile
- Common solution sets for security and IPsec functionality to support cross-agency security functionality

7.4   U.S. Government Configuration Baseline

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 United States Government Configuration Baseline (USGCB), 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 USGCB solutions:

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

7.5   Networx Migration

As of February 2012, GSA reports that over 97% of FTS-2001 telecommunications services have transitioned to the Networx set of contract vehicles. The target for final completion is December 2012. For the agencies that have completed the Networx transition, or those currently in process or being planned, the transition to Networx will be one of the greatest opportunities to implement IPv6 across their entire enterprise in a cost-effective manner. In June 2008, agencies were required to enable agency infrastructures (network backbones) to use IPv6. The experience acquired through these activities, along with the other associated activities, detailed throughout this document, can provide the agencies with the understanding and background required to successfully implement IPv6.

As agencies develop and refine their Networx requirements, they should do so in conjunction with their short- and long-term IPv6 plans to ensure that their Networx vendor can adequately support their requirements. This should include every aspect of the enterprise that is being impacted during the Networx transition, including the Trusted Internet Connection (TIC) Internet consolidation program, the United States Government Configuration Baseline (USGCB), the Cloud-First Policy and the Digital Government Strategy. IPv6 design should account for each of these initiatives and can build in the flexibility to adapt to additional requirements. By following network addressing best practices and specific IPv6 lessons learned, agencies can successfully implement and support the current initiatives while ensuring a solid foundation for future evolution and innovation.

During their Networx 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 address and network management
- IPv6 SLAs
- DNS support

OMB and GSA continue to hold on-going discussions with Networx and MTIPS providers to confirm the availability and readiness of IPv6 services. Agency transition managers are encouraged to participate in the discussions and to provide agency experiences with the acquisition and implementation of IPv6 services via the Networx contract. Transition Managers should also work with their appropriate Networx

Designated Agency Representatives (DAR) and their Network Operations group to proactively update their existing circuit inventory and to confirm the ability of all circuits to support IPv6.

GSA's Connections II offers IPv6-compliant equipment, applications, transition support, and integrated solutions to help you with your IPv6 conversion planning, including:

- Upgrade public/external facing servers and services (e.g. Web, email, DNS, ISP services, etc.) to operationally use native IPv6
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6
- Support your IPv6 Transition Manager in leading the agency's IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary
- Support agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities
- Connections II meets Federal agencies' equipment, labor, building, and campus infrastructure solution needs, including: Infrastructure design, installation, and implementation, Professional services to support existing networks, Transition planning and integration services, Customized client-specific systems

Connections II offers access to 21 pre-competed industry partners:

- A&T Systems, Inc.
- American Systems Corporation
- Apptis, Inc.
- AT&T Technical Services Company, Inc.
- Avaya Government, Solutions, Inc.
- BAE Systems Information Solutions, Inc.
- CIBER, Inc.
- Concert Technologies, Inc.
- EPS Corporation
- Futron, Inc.
- General Dynamics Information Technology, Inc.
- Government Telecommunications, Inc.
  Harris IT Services Corporation
- HP Enterprise Services, LLC
- Netcom Technologies, Inc.
- Nextira One Federal LLC d/b/a Black Box Network, Services
- Qwest Government Services, Inc. d/b/a Century Link QGS
- Science Applications International Corporation (SAIC)
- The Centech Group, Inc
- Vector Resources, Inc.
- Verizon Federal, Inc.

Further information for Ordering and Fair Opportunity is available: http://www.gsa.gov/portal/content/113287. Also, GSA Connection II staff can also help with Statement of Work (SOW) information and requests.

7.6 DNSSEC

Deployment of DNSSEC is continuing at a rapid pace as a number of the second level .gov domains have already been signed. Status of domains can be viewed at: http://www.dnsops.gov/USAdotGOV-status.html. With the increasing number and complexity of DNS queries for more complex Web sites with enhanced services, the performance of DNSSEC services securing the DNS resolving infrastructure is critical. A method to decouple DNS services during the initial transition phase is to add an IPv6 only overlay DNS server infrastructure along with existing IPv4 DNS servers. This will increase the load on the number of zones that need to get signed and potentially the PKI infrastructure to sign them. Customer facing DNS servers will not be authenticating customer queries but will be authenticated by the DNS infrastructure supporting those customer facing DNS servers. It is recommended that address management systems be used to automatically generate forward and reverse resource records (RR)s for DNS servers. DNSSEC authenticates Primary DNS server traffic out to end users and devices requesting URL resolution but not the systems generating the DNS RRs. Agencies should verify the security of the generation and transportation of DNS RRs to their primary DNS servers, meets their security requirements.

The processor intensive cryptographic requirements of DNSSEC will place additional load on the hardware and processors of the host servers or appliances. These systems should be sized correctly to handle peak and sustained loads under periods of network stress. DNS servers with DNSSEC and other processor intensive network services are not good candidates for virtualization, multi-role appliances or servers.

7.7 Cloud Computing: Cloud First Strategy

Due to the potential cost savings and overall improved performance capabilities, OMB has initiated a Cloud-First Strategy for agency applications and services that can migrate to a Cloud-based infrastructure. This can apply to public, private, or hybrid public-private clouds.

It is critical that agencies identify and incorporate IPv6 requirements at the beginning of the Cloud Computing efforts. IPv6 will play a pivotal role in the future and overall value of Cloud Computing solutions. At a minimum, agencies should ensure that their internal or external cloud service provider can provide the IPv6 capabilities necessary to meet their requirements for the 2012 and 2014 milestones and future IPv6 mission requirements.

7.8 Federal Data Center Consolidation Initiative (FDCCI)

FDCCI is a major initiative to reduce the number of data centers across the Federal Government. The expected result will be a decrease in overall cost, resources, space, and power consumption. This not only furthers the goal of a more efficient government, but a greener government as well.

IPv6 will play a critical role in developing the service-oriented infrastructure necessary to provide the fully virtualized computing and network environments for agencies to create next generation data centers that provide the flexibility and agility necessary to maximize their value in the FDCCI initiative.

Agencies should plan to accommodate IPv6 within the consolidated data center, paying special attention to security architecture and network management. IPv6 paths might provide inadvertent back doors or increase the likelihood of using an IPv6 network to exploit vulnerability on the IPv4 network.

7.9   Digital Government Strategy

Today's amazing mix of high performance servers, cloud computing, ever-smarter mobile devices, collaboration and sharing tools has the potential to fundamentally change the Government and its service delivery model. With ever expanding mission requirements and smaller budgets it is incumbent on agencies to review their service delivery methods and internal processes to better leverage the digital revolution which was the genesis for development of the Digital Government Strategy.

The Digital Government Strategy sets out to do two things:

- Enable citizens and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device. By operationalizing a data-centric model, we can architect our systems for interoperability and openness, modernize our content publication model, and deliver better digital services, at a lower cost, and in a platform and device agnostic way.

- Ensure that as the government adjusts to this new digital world, we seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways. Learning from the previous transition of moving information and services online, we now have an opportunity to break free from the inefficient, costly, and fragmented practices of the past, build a sound governance structure for digital services, and do mobile "right" from the beginning.

Additional information on the strategy is available on line at:
http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html ("Digital Government, Building a 21st Century Platform to Better Serve the American People")

8. IPv6 in IT Governance and Procurement

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

8.1   Governance

Agencies will need to update their Transition Plans to reflect the next steps in their IPv6 transition. This must 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 throughout the transition to ensure agency-wide participation.

Agencies should:

- Develop updated policies to support the on-going IPv6 transition activities, including:
    - Organizations stated 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

8.2   Procurement

One of the primary tenets of the Federal IPv6 transition philosophy is the use of technology refreshment cycles to enable IPv6 across the Federal-wide Enterprise Architecture. This concept supports an extended transition timeframe during which agencies can incorporate IPv6 into their normal acquisition cycles over time, thus reducing the need for large capital deployments to support the transition. With the new targets established by OMB for 2012 and 2014, some agencies may find that waiting for technology refresh will not be a compatible approach to meeting these dates. In these instances, agencies will need to direct short-term funds to ensure the necessary IPv6 functionality.

9. Contributors

This guide 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 Strategy and Planning Committee (SPC) of the Federal Chief Information Officer (CIO) Council. The E-Government Act of 2002 authorizes the Federal CIO Council. This guide was developed in conjunction with the American Council for Technology/Industry Advisory Council.

The following SPC and TIS leadership members and OMB staff were responsible for the development of this guide:

Name	Roles	Title	Organization
Simon Szykman	Co-Chair , Strategy and Planning Committee (SPC)	CIO	Department of Commerce (DoC)
Linda Cureton	Co-Chair, SPC	CIO	NASA
Roberta Stempfley	Co-Chair, Technology Infrastructure Subcommittee (TIS)	Deputy Assistant Secretary, National Protection & Programs Directorate	Department of Homeland Security (DHS)
Charles Romine	Co-Chair, Technology Infrastructure Subcommittee (TIS)	Director ITL	Department of Commerce (DoC), National Institute of Standards and Technology, Information Technology Laboratory
Peter Tseronis	Chair, Federal IPv6 Task Force	Chief Technology Officer	Department of Energy (DoE)
Bobby Flaim	Co-Chair, Federal IPv6 Task Force	Supervisory Special Agent	Department of Justice (DoJ), Federal Bureau of Investigations (FBI)
Carol Bales	Executive Sponsor	Lead Policy Analyst	Executive Office of the President (EoP) Office of Management and Budget

The following persons were primary contributors to developing this guide:

Name	Roles	Title	Organization
Chris Chroniger	Chair – ACT-IAC IPv6 Working Group	Chief Technology Officer	Acentia
Jane Coffin	Key Contributor	Policy Analyst	Department of Commerce (DoC)
Dale Geesey	Key Contributor	Chief Operating Officer	Auspex Technologies
John L. Lee	Key Contributor	Chief Technology Officer	Internet Associates LLC
Kenny Burroughs	Key Contributor	Managing Director	Internet Associates LLC
Barry Chapman	Key Contributors	Solutions Architect	Acentia
Ralph Wallace	Key Contributor	President/Owner	White Oak Consulting LLC
Doug Montgomery	Key Contributor	Manager, Internetworking Technologies Research Group	Department of Commerce (DoC) NIST
Stephen Nightingale	Key Contributor	Senior Computer Scientist	Department of Commerce (DoC) NIST
Ron Broersma	Key Contributor	Chief Engineer	Department of Defense (DoD) DREN
Tim Owen	Key Contributor	Chief Engineer	Secure Mission Solutions

Name	Roles	Title	Organization
TJ Evans	Key Contributor	Director, Network Engineering	Nephos6
Bill Kyburz	Key Contributor	Senior Director, Business Development	General Dynamics
Joe Klein	Key Contributor	Cyber Security Principal Architect	QinetiQ, North America

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

Name	Organization
Steven Pirzchalski	Department of Veterans Affairs (VA)
Silvia Brugge	Acentia
Kafi Johnson	Acentia
Frank Troy	Troy Networks, Inc.
Wendy Fox	Long Boat, LLC

10. Acronym Dictionary

Acronym	Description
AAAA	Authentication, authorization, accounting and auditing
ACL	Access control list
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
BGP	Boundary Gateway Protocol
CAFEA	The Common Approach to Federal Enterprise Architecture
CCTV	Closed Circuit Television
CDN	Content Delivery Network
CIDR	Classless Inter Domain Routing
COI	Communities of Interest
CONUS	Continental United States
COOP	Continuity of Operations Plan
CPIC	Capital Planning and Investment Control
DARPA	Defense Advanced Research Projects Agency
DCID	Director of Central Intelligence Directives
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DISR	DoD Information Standards Registry
DMZ	Demilitarized Zone
DDNS	Dynamic DNS
DNS	Domain Name System
DNSSEC	Domain Name System (DNS) Security Extensions
DoD	Department of Defense
DOL	Department of Labor
DOT	Department of Transportation
EA	Enterprise Architecture
EAAF	Enterprise Architecture Assessment Framework
E-Authentication	Electronic Authentication
ED	Education
E-Mail	Electronic Mail
e-Gov	Electronic Government
FDCC	Federal Desktop Core Configuration
FEA PMO	Federal Enterprise Architecture Program Management Office
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HSPD-12	Homeland Security Presidential Directive-12
IA	Information Assurance
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IP Fax	Internet Protocol Facsimile
IPAM	Internet Protocol Address Management
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPT	Internet Protocol Telephony

Acronym	Description
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISC	Internet Systems Consortium
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
IT	Information Technology
ITI LoB	Information Technology (IT) Infrastructure Line of Business
ITI PPMO	IT Infrastructure Program Performance Measurement Office
ITS	Intelligent Transportation Systems
ITV	In-Transit Visibility
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
LoB	Line of Business
MAC ID	Media Access Control Identification. (MAC is also known as Medium Access Control.)
MIPv6	Mobile IP version 6
MPLS	Multi-Protocol Label Switching
NA	Neighbor Advertisement
NAC	Network Access Control
NADM	Network Admission Control
NAT	Network Address Translation
ND	Neighbor Discovery
NDP	Neighbor Discovery Protocol
NEMO	Network Mobility
NIST	National Institute for Standards and Technology
NMS	Network Management System
NOAA	National Oceanic and Atmospheric Administration
NS	Neighbor Solicitation
NWS	National Weather Service
OMB	Office of Management and Budget
OOB	Out of Band (Management)
OS	Operating System
OSPF	Open Shortest Path First
P2P	Peer to (2) Peer
PAT	Port Address Translation
PCs	Personal Computers
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PoC	Point of Contact
QoS	Quality of Service
RA	Router Advertisement
RFC	Request for Comments
RFP	Request for Proposal
RIR	Regional Internet Registry
RR	(DNS) Resource Record
SCIF	Sensitive Compartmented Information Facility
SEND	SEcure Neighbor Discovery

Acronym	Description
SLAAC	Stateless Address Auto Configuration
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TIC	Trusted Internet Connection
TRM	Time Reversal Mirror
TSIG	Transaction SIGnature
UC	Unified Communications
USGCB	United States Government Configuration Baseline
USG IPv6 FAQs	United States Government IPv6 Frequently Asked Questions
USPS	United.States Postal Service
VLAN	Virtual LAN
VoIP	Voice over Internet Protocol (IP)
VPN	Virtual Private Network
WAAS	Wide Area Application Services
WAN	Wide Area Network
WOA	Web Platform Oriented Architecture
WWW	World Wide Web

11. Definitions

- **Capital Planning and Investment Control** (**CPIC**): Means the same as capital programming and is a decision-making process for ensuring IT investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. The term comes from the Clinger-Cohen Act of 1998 and generally is used in relationship to IT management issues.
- **HSPD-12:** Homeland Security Presidential Directive (HSPD) 12 is "Policy for a Common Identification Standard for Federal Employees and Contractors"
- **NETWORX:** Federal Government contract vehicle for telecommunications and related services.

12. IPv6 FAQ

The Federal IPv6 task force has created and maintains a set of Frequently Asked Questions that are published on the CIO.GOV Website at the URL below:

http://www.cio.gov/Documents/IPv6-FAQ%2011-4-2011.pdf

13. Resources

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

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

IPv6 FAR Amendment
http://www.gpo.gov/fdsys/pkg/FR-2009-12-10/pdf/E9-28931.pdf

"IPv6 Standards Profile Released," September 19, 2008.
http://gcn.com/articles/2008/09/19/ipv6-standards-profile-released.aspx

IPv6 Wiki for Transition Managers
https://max.omb.gov/community/x/EhPVI

NIST IPv6 Deployment Monitor
http://fedv6-deployment.antd.nist.gov/

NIST SP800-119 "Guidelines for the Secure Deployment of IPv6, December 2010
http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

"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

NIST USGv6 Deployment Test Suite
http://www.antd.nist.gov/usgv6/

NTIA IPv6 Web-page and Resources
http://www.ntia.doc.gov/category/ipv6

"OMB: Agencies met IPv6 deadline," July 1, 2008.
http://fcw.com/Articles/2008/07/01/OMB-Agencies-met-IPv6-deadline.aspx

Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government
http://www.cio.gov

Practical Guide on Federal Service Oriented Architecture, June 2008.
http://www.whitehouse.gov/omb/E-Gov/pgfsoa

September 28, 2010 OMB Memorandum
http://www.cio.gov/documents/IPv6MemoFINAL.pdf

"Service-Oriented Infrastructure Project Description," July 31, 2007
http://www.docstoc.com/docs/75121434/Service-Oriented-Infrastructure-Project-Description-%E2%80%9CFrom-

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

For a summary of the relevant amendments, refer to:
http://edocket.access.gpo.gov/2009/pdf/E9-28931.pdf