U.S. Department of Education

Enterprise Architecture Program Office (EAPO)

IPv6 Transition Guide

Version 2.0

April 18, 2011

Revision History

Version	Comments	Date
0.1	Initial Version	October 20, 2009
0.2	Changed Overall Structure and Purpose per Joe Rose and Milestone Plan Content per Steven Corey-Bey	October 30, 2009
0.3	• Changed part of document title from “Implementation Roadmap” to “Transition Guidance”. • Changed Date of document from October 30, 2009 to November 19, 2009. • Changed “Responsibilities” to “Responsibilities and Scope”. • Changed “Policy” to “Transition Guidance”. • Decreased outline level of “Testing Considerations” section. • Capitalized “Internet Protocol” on p.4. • Added outline labels to sections. • Copied owner information from IPv6 Transition Milestones table in for tables in “Transition… • Added words to IPv6 Working Group introductory paragraph. • Deleted two sentences from Transition Guidance .introductory paragraph. Modified remaining sentence. • Deleted Appendix.	November 11, 2009
1.0	• Changed title page portion from “Guidance” to “Guide” • Changed title page summary from “governance” to “guidance” • Changed title page date from “19” to “30” • On page 4, added references for IP Guidance • On page 5, removed extra open parenthesis • On page 6 deleted 2 sentences, two phrases, added words as appropriate to maintain coherence. Bold-faced transition stages and IT groups • On page 7, enabled borders for table 5 and added description for table 6 • On page 9, added PIRWG reference to section 3.1 bullet list. Modify 9 sentences with minor word exchanges, additions, or deletions such as replacing “one or more” with “several”. • On page 10, modified 4 sentences in the first 3 paragraphs and added a sentence to the 3rd paragraph. • On page 11, changed first sentence of first paragraph into two sentences. Deleted last paragraph, except for its last sentence. Modified that last sentence. Added Table 8 reference source. • On page 12, italicized reference source. Deleted several sentences in first two paragraphs. Made minor changes to remaining sentences. • On page 13, deleted several sentences in first two paragraphs. Made minor changes to remaining sentences. • On page 14, deleted all paragraphs and add one sentence to carryover paragraph from page 13.	November 13,2009
1.1	• Delete Training Needs Analysis (12/2009) to Table 7 IPv6 Transition Milestones & Table 4 OCIO-EA • Added Complete IPv6 upgrade inventory list (02/2010) to Table 7 IPv6 Transition Milestones & Table 2 Application Owners	January 8, 2010
1.2	• Updated the transition schedule, activities and milestones. • Changed transition schedule to include separate tasks for internal and external facing servers and services	March 18, 2011
2.0	• Updated document layout to adhere to EA Chief Architect transition plan guidance • Updated schedule based on executive feedback	March 30, 2011

Table of Contents

1. Purpose and Strategic Objective

The purpose of this document is to describe the purpose and approach to accomplishing the Internet Protocol version 6 (IPv6) transition milestones.

1.1. IPv6 Overview

Use of the Internet is critical to the Department of Education to the performance of its mission and delivery of services to citizens. The Internet enables collaboration and communication between people, organizations and systems worldwide. The primary communications protocol of the Internet since its inception in the 1970's is the *Transmission Control Protocol/Internet Protocol TCP/IP*. This term was shortened to Internet Protocol, or "IP". IP version 4 (IPv4) is the primary Internet protocol in use today. IPv4 provided up to four billion unique IP addresses for use on the Internet. At the time of its invention, designers thought IPv4 provided all the Internet addresses we would ever need. The explosive growth and demand by people, systems and devices for IP addresses to access the Internet has exceeded the limits of TCP/IP's original design. IP version 6 (IPv6) is the next generation protocol for the Internet.

The complete transition of the global Internet from IPv4 to IPv6 is expected to span many years. During this period of transition, the Department will operate in a "dual-stack" network environment, supporting IPv4 and IPv6 concurrently, possibly for the foreseeable future. The incremental, phased deployment approach allows for a significant period where IPv4 and IPv6 can co-exist using one or more transition mechanisms to ensure interoperability between the two protocol suites.

1.2. IPv6 Features and Business Benefits

In response to impending exhaustion of IPv4 addresses the Internet Engineering Task Force (IETF) began developing and enhanced version of TCP/IP that we now call IPv6. With its 128-bit address space, IPv6 was designed to support continued Internet growth, both in terms of the number of users and available functionality. It is expected to overcome other IPv4 limitations through features such as end-to-end IP Security (IPSec) support, mobile communications, Quality of Service (QoS), and other features that are designed to ease system and network management burdens.

The main advances from IPv4 to IPv6 are:

- Expanded addressing capability,
- Security extensions for authentication and privacy,
- Flow labeling capability,
- Improved efficiency in routing and packet handling,
- Support for auto-configuration and plug-and-play capabilities,
- Support for embedded IP Security,
- Elimination of the need for Network Address Translation (NAT),
- Support for widely deployed routing protocols, and
- Network efficiency and bandwidth conservation.

Additionally, IPv6 includes transition and interoperability mechanisms that allow users to deploy IPv6 incrementally.

1.3. IPv6 Challenges

The following challenges should be considered from each agency's program perspective in the development of the IPv6 transition plan.

1.3.1. Maintaining interoperability and security during transition

The Department will need to maintain network interoperability as they transition away from today's IPv4-only environment. During the initial phases of transition, the Department will move to an environment that accommodates native IPv6 and encapsulated IPv6, in a largely IPv4 network leading to a ubiquitous dual-stack environment. As applications transition and the use of IPv4 diminish, the Department will operate in an environment largely as an IPv6 network. Hardware and software interoperability will be essential as the Department moves forward with their IPv6 plans and interconnect its network across dual environments. Since maintaining interoperability and security for these types of evolving environments is the highest priority, the transition period will be kept minimized. Furthermore, there will be an on-going need for interaction with IPv4 enclaves outside of the agency requiring transition mechanisms to be planned accordingly.

1.3.2. IPv6 Standards and Product Evolution

Today, IPv6 technology is still evolving and this evolution is likely to continue through the federal transition period. This evolution is common of the Internet standards. While the base set of IPv6 protocols are stable and mature, and product implementations are emerging, many of the standards supporting value-added IPv6 features are still evolving. Therefore, this plan will identify the plan the Department will use ensure the IPv6 capabilities being procured have a viable upgrade path.

1.4. Background and References

In 2006, the Office of Management and Budget (OMB) began to use the Enterprise Architecture Assessment Framework to evaluate the Department's IPv6 transition planning and progress, IP device inventory completeness, and impact analysis thoroughness. In June 2008, the Department successfully exchanged IPv6 network traffic with an external IPv6 network, which identified the Department's network as being IPv6 "capable." In September 2010, OMB issued an updated memorandum extending the capability requirements of the network, indicating all external-facing servers and services were to be IPv6 capable by 2012. Internal-facing servers and services were to follow, being IPv6 capable by 2014. The memorandum also established a task force to guide Federal agencies in the transition process. This transition plan outlines the IPv6 transition activities and milestones, a strategy to complete those activities and milestones and the governance activities surrounding those transition activities.

This IPv6 Transition Plan is based on the following references:

Document Title	Document Number	Organization
Transition to IPv6 Memorandum	September 28, 2010	Vivek Kundra, Federal CIO
Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government	May 2009 version 1.0	The Federal CIO Council Architecture and Infrastructure Committee, Technology Infrastructure Subcommittee, Federal IPv6 Working Group
NIST Profile for IPv6 in the U.S. Government – Version 1.0	NIST SP 500-267A	National Institute of Standards and Technology (NIST)
Federal Acquisition Regulation	(FAR) 11.002(g)	General Services Administration (GSA)
Enterprise Architecture Assessment Framework	Versions 2.x to 3.x	Office of Management and Budget (OMB)
An Internet Transition Plan	RFC-5211	(Internet Engineering Task Force) IETF
General Requirements for the Competence of Testing and Calibration Laboratories	ISO 17025	Internal Standards Organization(ISO)
Guidance on IPv6 Test Methods and Validation	NIST SP 500-273	National Institute of Standards and Technology (NIST)
Integrating IT Security into the Capital Planning and Investment Control Process	NIST SP 800-65	National Institute of Standards and Technology (NIST)

2. Transition Activities and Milestones

The Department's IPv6 Transition is integrated into the Department's EA Transition Strategy. The Department's deployment of IPv6 covers five transition phases for two distinct network environments.

The five transition phases are:

- **Inventory**
- **Assessment**
- **Remediation**
- **Testing**
- **Implementation**

These five transition phases are implemented in two implementation cycles – one for externally-facing Internet applications and systems and one for internal applications, servers and systems that access the Internet.

Within each transition stage, the milestones are grouped by **Infrastructure, Applications,** and **Governance**. Within each of these groups, activities are associated with owners and milestone dates. As the Department becomes aware of any additional IPv6 requirements and schedule changes, this Transition Guide will be updated. Please contact the Agency IPv6 Transition Manager to request the current IPv6 Schedule.

The following sections describe the enterprise view of tasks (first for externally-facing applications, servers and systems, then internally-facing). Following the enterprise tasks, the subsequent sub-sections describe the specific tasks by owner within the Department. The owners in the tasks are identified as:

2.1. Externally-facing Servers and Services Activities and Milestones

	Task Force Phase	Group	Activities	Milestones	Owner	Milestone Date
Externally-Facing Servers/Services/Applications/Systems	Inventory 10/2010 -5/2011	Application	Develop IPv6 inventory that includes the IP (IPv4, 6, dual) and retirement status of external-facing applications	IPv6 inventory data call to POC	Application Owner	3/30/2011
		Application	Submit funding requests for select phase to POC.	Non-major data call, Select Presentations	Application Owner	4/30/2011
		Application	Develop high-level transition milestones for external apps	IPv6 data call Update	Application Owner	5/1/2011
		Governance	Appoint Agency Transition Manager	Appointment of Agency Transition Manager	OCIO-EA	10/30/2010
		Governance	Establish an internal tiger team reporting to the CIO	Internal Tiger Team meeting notes	OCIO-EA	3/30/2011
		Governance	Update IPv6 Transition Plan	Updated IPv6 Transition Plan	OCIO-EA	4/30/2011
		Infrastructure	Identify a website for enablement (www.ed.gov)	IPv6 enabled website	OCIO-ITS	3/30/2011
		Infrastructure	IPv6 service request completed	IPv6 service	OCIO-ITS	5/15/2011
		Infrastructure	Develop inventory of network components that support external systems.	Updated Inventory List	OCIO-ITS	4/30/2011
		Infrastructure	Determine requirement for IPv6 test lab	Test lab requirements	OCIO-ITS	4/30/2011
		Infrastructure	Submit funding requests for select phase to POC.	Non-major data call, Select Presentations	OCIO-ITS	5/16/2011
		Infrastructure	Develop IPv6 Addressing, Network Management, and Testing Plan	IPv6 Addressing Plan, Network Management Plan, Testing Plan	OCIO-ITS	5/30/2011
		Infrastructure	Begin inventory of agency Mail Exchanges (MX)	MX Inventory	OCIO-ITS	5/30/2011
	Assessment 4/2011 - 9/2011	Application	Certify external apps for IPv4, IPv6 or Dual Stack Capability	IPv6 inventory data call to POC	Application Owner	4/30/2011
		Application	Examine external applications for IPv4 dependency	IPv4 dependency report	Application Owner	8/30/2011
		Application	Prioritize external applications for upgrades or retirement	Priority list	Application Owner	6/30/2011
		Application	Develop Transition and Remediation Plans for external applications	Transition Strategy, Remediation Plan (per application or system)	Application Owner	8/30/2011
		Governance	Participate in World IPv6-day	Participation	OCIO-EA	6/8/2011
		Governance	Record the agency's first public ipv6-enabled web site	IPv6 Web Site AAAA record	OCIO-EA	6/8/2011
		Governance	Begin research, develop, & vet security concerns	Security report on IPv6	OCIO-IA	9/30/2011
		Governance	Begin development of IPv6 security policy	Security policy document	OCIO-IA	9/30/2011
		Governance	Begin development of IPv6 security procedures	Security procedures document	OCIO-IA	9/30/2011
		Governance	Begin development of IPv6 security technical implementation guides (STIG)	STIGs for network devices	OCIO-IA	9/30/2011
		Infrastructure	Develop Test Lab Requirements and budget requests	Requirements document, POC budget request	OCIO-ITS	7/1/2011
		Infrastructure	Enable IPv6 Web server (www.ed.gov)	IPv6 Web server (www.ed.gov) enabled	OCIO-ITS	5/15/2011
		Infrastructure	Establish one (mininum) DNS server with AAAA record	Authoratative DNS with AAAA record	OCIO-ITS	5/15/2011
		Infrastructure	Examine MX for IPv4 dependency	IPv4 dependency report	OCIO-ITS	7/1/2011
		Infrastructure	Ensure addressing plan ready to implement	Addressing plan certification	OCIO-ITS	6/30/2011
		Infrastructure	Prioritize network components for upgrade or retirement	Priority list	OCIO-ITS	8/30/2011
		Infrastructure	Develop Transition and Remediation Plans for network components	Transition Strategy, Remediation Plan	OCIO-ITS	8/30/2011

	Remediation 4/2011 - 4/2012	Application	Begin upgrade of external applications to support IPv6	Application upgrade	Application Owner	8/30/2011
		Application	Develop an application Test Plan	Test plan	Application Owner	4/30/2012
		Governance	Update Transition Plan	Updated Transition Plan	OCIO-EA	9/30/2011
		Governance	Begin deployment of IPv6 security procedures	Security procedures document	OCIO-IA	10/1/2011
		Governance	Identify additional public services and services, including sub-agencies	Updated URL List	OCIO-EA	12/30/2011
		Governance	Begin support staff, operations and security staff training	Training class	OCIO-EA	4/30/2012
		Infrastructure	Finalize plan for DNS, review IPSec signing to include AAAA records	Updated DNS Plan	OCIO-ITS	9/30/2011
		Infrastructure	Begin deployment of IPv6 security technical implementation guides (STIG)	implemented STIGs in configurations of network devices	OCIO-ITS	10/1/2011
		Infrastructure	Prioritize MX for upgrades or retirement	MX Upgrade Plan	OCIO-ITS	9/30/2011
		Infrastructure	Upgrade MX components to support IPv6	MX component upgrade certification	OCIO-ITS	9/30/2011
			Upgrade DNS to support IPv6		OCIO-ITS	9/30/2011
		Infrastructure	Authoritative DNS servers to provide transport over IPv6	IPv6 Transport validated	OCIO-ITS	12/30/2011
		Infrastructure	Upgrade network components to support IPv6		OCIO-ITS	12/30/2011
	Testing 5/2012-8/2012	Application	Begin testing IPv6 applications	Test Plan Results	Application Owner	5/30/2012
		Application	Certify operation of needed IPv4 applications on network	Test Plan Results	Application Owner	8/30/2012
			Certify external-facing applications as IPv6 Operational	Test Plan Results	Application Owner	8/30/2012
		Application	Certify external-facing applications as Dual Stack Operational	Test Plan Results	Application Owner	8/30/2012
		Governance	Update Transition Plan	Updated Transition Plan	OCIO-EA	8/30/2012
		Infrastructure	Test Lab in Place	Test Lab	OCIO-ITS	5/1/2012
		Infrastructure	Begin testing IPv6 systems	Test Plan Results	OCIO-ITS	5/30/2011
			Certify external/public-facing servers as IPv6 Operational	Security Authorization	OCIO-ITS	8/30/2012
		Infrastructure	Certify external/public-facing servers as Dual Stack Operational		OCIO-ITS	8/30/2012
	Implementation 9/2012 - 10/2012	Application	Deploy external-facing IPv6 Applications	Security Authorization	Application Owner	9/30/2012
		Application	Begin decommission of IPv4 applications as needed	Updated IPv6 inventory data call	Application Owner	10/1/2012
		Infrastructure	Implementation IPv6 systems	Security Authorization	OCIO-ITS	9/30/2012
		Infrastructure	Begin Decommission of IPv4 Nodes asneeded	Updated IPv6 inventory data call	OCIO-ITS	10/1/2012
		Governance	Validate upgrade of public/external facing servers	IPv6 report to OMB, updated Transition Plan	OCIO-EA	10/1/2012

2.2. Internally-facing Servers and Services Activities and Milestones

	Task Force Phase	Group	Activities	Milestones	Owner	Milestone Dates
Internally-Facing Servers/Services/Applications/Systems	Inventory 3/2012-9/2014	Application	Develop IPv6 inventory that includes the IP (IPv4, 6, dual) and retirement status of external-facing applications	IPv6 inventory data call to POC	Application Owner	3/10/2012
		Application	Submit funding requests for select phase to POC	Non-major data call, Select Presentations	Application Owner	5/30/2012
	Assessment 6/2012-9/2012	Application	Examine applications for IPv4 dependency	IPv4 dependency report	Application Owner	7/30/2012
		Application	Prioritize applications for upgrades or decommissioning	Priority List	Application Owner	7/30/2012
		Application	Develop Transition Strategy and Remediation Plan	Transition Strategy and Remediation Plans (per application or system)	Application Owner	7/30/2012
		Governance	Research, develop, & vet security concerns	Security report on IPv6 (internal-facing)	OCIO-IA	6/30/2012
		Governance	Develop IPv6 security procedures	STIGs	OCIO-IA	6/30/2012
		Governance	Update Transition Plan (co-incides with update for external-facing)	Updated Transition Plan	OCIO-EA	9/30/2012
		Governance	Procurement policy updated for internal applications	Updated procurement policy for IPv6	CAMS	9/30/2012
		Infrastructure	Examine applications for IPv4 dependency	IPv4 dependency report	OCIO-ITS	7/30/2012
		Infrastructure	Prioritize applications for upgrades or decommissioning	Priority List	OCIO-ITS	7/30/2012
		Infrastructure	Update addressing plan for internal-facing applications	Updated addressing plan	OCIO-ITS	6/30/2012
		Infrastructure	Update Transition and Remediation Plans if necessary	Updated Transition, Remediation Plans	OCIO-ITS	8/30/2012
	Remediation 9/2012 to 7/2013	Application	Develop Test Plan	Test Plan	Application Owner	9/30/2012
		Application	Upgrade applications to support IPv6	Updated IPv6 inventory data call to POC	Application Owner	7/30/2013
		Infrastructure	Develop Test Plan	Test Plan	OCIO-ITS	9/30/2012
		Infrastructure	Upgrade applications to support IPv6	Updated IPv6 inventory data call to POC	OCIO-ITS	7/30/2013
	Testing 7/2013-8/2014	Application	Test IPv6 applications	Test Plan results	Application Owner	7/30/2014
		Application	Certify operation of needed IPv4 applications on network	Test Plan results	Application Owner	8/30/2014
		Application	Certify internal facing applications as IPv6 Operational	Test Plan results	Application Owner	8/30/2014
		Infrastructure	Ensure test lab is available for internal application testing	Test Lab	OCIO-ITS	7/30/2013
	Implementation 9/2014	Application	Implement Internal-facing IPv6 Applications	Test Plan Results	Application Owner	9/30/2014
		Application	Begin decommission of IPv4 applications as needed	Updated IPv6 inventory data call	Application Owner	9/30/2014
		Infrastructure	Implement Internal-facing IPv6 Applications	Test Plan Results	OCIO-ITS	9/30/2014
		Infrastructure	Begin decommission of IPv4 applications as needed	Updated IPv6 inventory data call	OCIO-ITS	9/30/2014
		Governance	Validate upgrade of internal-facing applications for IPv6	IPv6 report to OMB, updated Transition Plan	OCIO-EA	9/30/2014

2.3. Application Owner-Specific Activities and Milestones

Activities and milestones, derived from enterprise view of activities are filtered for application owner activities into the following two tables:

Application Owner Activities

	Activities	Milestones	Milestone Dates
Externally Facing Applications, Systems	Develop IPv6 inventory that includes the IP (IPv4, 6, dual) and retirement status of external-facing applications	IPv6 inventory data call to POC	3/30/2011
	Submit funding requests for select phase to POC.	Non-major data call, Select Presentations	4/30/2011
	Develop high-level transition milestones for external apps	IPv6 data call Update	5/1/2011
	Certify external apps for IPv4, IPv6 or Dual Stack Capability	IPv6 inventory data call to POC	4/30/2011
	Examine external applications for IPv4 dependency	IPv4 dependency report	8/30/2011
	Prioritize external applications for upgrades or retirement	Priority list	6/30/2011
	Develop Transition and Remediation Plans for external applications	Transition Strategy, Remediation Plan (per application or system)	8/30/2011
	Begin upgrade of external applications to support IPv6	Application upgrade	8/30/2011
	Develop an application Test Plan	Test plan	4/30/2012
	Begin testing IPv6 applications	Test Plan Results	5/30/2012
	Certify operation of needed IPv4 applications on network	Test Plan Results	8/30/2012
	Certify external-facing applications as IPv6 Operational	Test Plan Results	8/30/2012
	Certify external-facing applications as Dual Stack Operational	Test Plan Results	8/30/2012
	Deploy external-facing IPv6 Applications	Security Authorization	9/30/2012
	Begin decommission of IPv4 applications as needed	Updated IPv6 inventory data call	10/1/2012
Internally-facing Applications, Systems	Develop IPv6 inventory that includes the IP (IPv4, 6, dual) and retirement status of external-facing applications	IPv6 inventory data call to POC	3/10/2012
	Submit funding requests for select phase to POC	Non-major data call, Select Presentations	5/30/2012
	Examine applications for IPv4 dependency	IPv4 dependency report	7/30/2012
	Prioritize applications for upgrades or decommissioning	Priority List	7/30/2012
	Develop Transition Strategy and Remediation Plan	Transition Strategy and Remediation Plans	7/30/2012
	Develop Test Plan	Test Plan	9/30/2012
	Upgrade applications to support IPv6	Updated IPv6 inventory data call to POC	7/30/2013
	Test IPv6 applications	Test Plan results	7/30/2014
	Certify operation of needed IPv4 applications on network	Test Plan results	8/30/2014
	Certify internal facing applications as IPv6 Operational	Test Plan results	8/30/2014
	Implement Internal-facing IPv6 Applications	Test Plan Results	9/30/2014
	Begin decommission of IPv4 applications as needed	Updated IPv6 inventory data call	9/30/2014

2.4. OCIO Enterprise Architecture-Specific Activities and Milestones

Activities and milestones, derived from enterprise view of activities are filtered for OCIO Enterprise Architecture-owned activities into the following two tables:

OCIO-EA Activities

	Activities	Milestones	Milestone Dates
Externally Facing	Appoint Agency Transition Manager	Appointment of Agency Transition Manager	10/30/2010
	Establish an internal tiger team reporting to the CIO	Internal Tiger Team meeting notes	3/30/2011
	Update IPv6 Transition Plan	Updated IPv6 Transition Plan	4/30/2011
	Participate in World IPv6-day	Participation	6/8/2011
	Record the agency's first public ipv6-enabled web site	IPv6 Web Site AAAA record	6/8/2011
	Update Transition Plan	Updated Transition Plan	9/30/2011
	Begin deployment of IPv6 security procedures	Security procedures document	10/1/2011
	Identify additional public services and services, including sub-agencies	Updated URL List	12/30/2011
	Begin support staff, operations and security staff training	Training class	4/30/2012
	Update Transition Plan	Updated Transition Plan	8/30/2012
	Validate upgrade of public/external facing servers	IPv6 report to OMB, updated Transition Plan	10/1/2012
Internally-facing	Update Transition Plan (co-incides with update for external-facing)	Updated Transition Plan	9/30/2012
	Validate upgrade of internal-facing applications for IPv6	IPv6 report to OMB, updated Transition Plan	9/30/2014

2.5. OCIO Information Assurance Services-Specific Activities and Milestones

Activities and milestones, derived from enterprise view of activities are filtered for OCIO Information Assurance Services-owned activities into the following table. These activities are to cover guidance, policy and planning for externally- and internally-facing applications, servers and services at the Department:

OCIO-IA Activities

	Activities	Milestones	Milestone Dates
Externally Facing	Begin research, develop, & vet security concerns	Security report on IPv6	9/30/2011
	Begin development of IPv6 security policy	Security policy document	9/30/2011
	Begin development of IPv6 security procedures	Security procedures document	9/30/2011
	Begin development of IPv6 security technical implementation guides (STIG)	STIGs for network devices	9/30/2011
	Begin deployment of IPv6 security procedures	Security procedures document	10/1/2011
Internally-facing	Research, develop, & vet security concerns	Security report on IPv6 (internal-facing)	6/30/2012
	Develop IPv6 security procedures	STIGs	6/30/2012

2.6. Contracts and Acquisition Management Services-Specific Activities and Milestones

The Department's Contracts and Acquisition Management Services (CAMS) is expected to fully updated its procurement policy with IPv6 requirements for all internally and externally-facing applications, servers and services. These updates are to cover guidance, policy and planning for any network-related tasks or services.

CAMS Activities

Activities	Milestones	Milestone Dates	Actual Dates
Procurement policy updated for internal applications	Updated procurement policy for IPv6	9/30/2012	

2.7. OCIO Information Technology Services-Specific Activities and Milestones

The following table filters OCIO Information Technology Services-owned activities for external and internal implementations:

OCIO-Information Technology Services (ITS) Activites

	Activities	Milestones	Milestone Dates
Externally Facing Servers/Services	Identify a website for enablement (www.ed.gov)	IPv6 enabled website	3/30/2011
	IPv6 service request completed	IPv6 service	5/15/2011
	Develop inventory of network components that support external systems.	Updated Inventory List	4/30/2011
	Determine requirement for IPv6 test lab	Test lab requirements	4/30/2011
	Submit funding requests for select phase to POC.	Non-major data call, Select Presentations	5/16/2011
	Develop IPv6 Addressing, Network Management, and Testing Plan	IPv6 Addressing Plan, Network Management Plan, Testing Plan	5/30/2011
	Begin inventory of agency Mail Exchanges (MX)	MX Inventory	5/30/2011
	Develop Test Lab Requirements and budget requests	Requirements document, POC budget request	7/1/2011
	Enable IPv6 Web server (www.ed.gov)	IPv6 Web server (www.ed.gov) enabled	5/15/2011
	Establish one (mininum) DNS server with AAAA record	Authoratative DNS with AAAA record	5/15/2011
	Examine MX for IPv4 dependency	IPv4 dependency report	7/1/2011
	Ensure addressing plan ready to implement	Addressing plan certification	6/30/2011
	Prioritize network components for upgrade or retirement	Priority list	8/30/2011
	Develop Transition and Remediation Plans for network components	Transition Strategy, Remediation Plan	8/30/2011
	Finalize plan for DNS, review IPSec signing to include AAAA records	Updated DNS Plan	9/30/2011
	Begin deployment of IPv6 security technical implementation guides (STIG)	implemented STIGs in configurations of network devices	10/1/2011
	Prioritize MX for upgrades or retirement	MX Upgrade Plan	9/30/2011
	Upgrade MX components to support IPv6	MX component upgrade certification	9/30/2011
	Upgrade DNS to support IPv6		9/30/2011
	Authoritative DNS servers to provide transport over IPv6	IPv6 Transport validated	12/30/2011
	Upgrade network components to support IPv6		12/30/2011
	Test Lab in Place	Test Lab	5/1/2012
	Begin testing IPv6 systems	Test Plan Results	5/30/2011
	Certify external/public-facing servers as IPv6 Operational	Security Authorization	8/30/2012
	Certify external/public-facing servers as Dual Stack Operational		8/30/2012
	Implementation IPv6 systems	Security Authorization	9/30/2012
	Begin Decommission of IPv4 Nodes asneeded	Updated IPv6 inventory data call	10/1/2012
Internally Facing Servers/Services	Examine applications for IPv4 dependency	IPv4 dependency report	7/30/2012
	Prioritize applications for upgrades or decommissioning	Priority List	7/30/2012
	Update addressing plan for internal-facing applications	Updated addressing plan	6/30/2012
	Update Transition and Remediation Plans if necessary	Updated Transition, Remediation Plans	8/30/2012
	Develop Test Plan	Test Plan	9/30/2012
	Upgrade applications to support IPv6	Updated IPv6 inventory data call to POC	7/30/2013
	Ensure test lab is available for internal application testing	Test Lab	7/30/2013
	Implement Internal-facing IPv6 Applications	Test Plan Results	9/30/2014
	Begin decommission of IPv4 applications as needed	Updated IPv6 inventory data call	9/30/2014

3. Transition Criteria for Legacy, Upgraded and New Capabilities

The Department's IPv6 transition manager will collect the following information for all applications, systems and services at the Department.

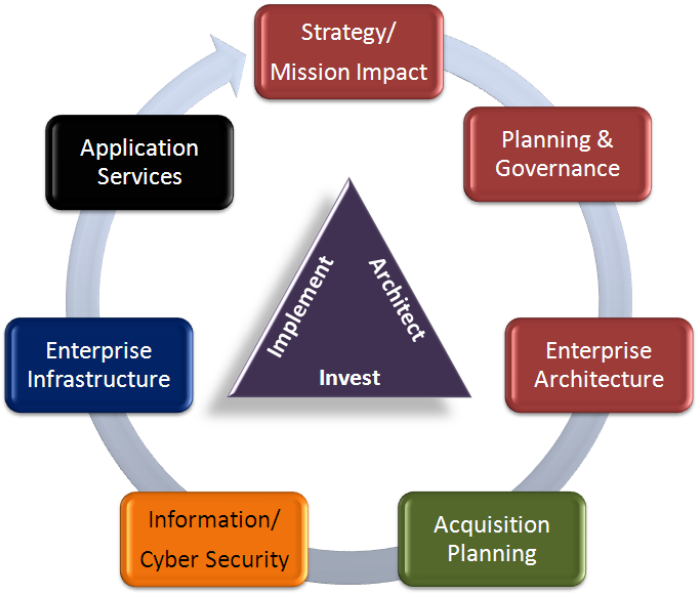
- **System Point of Contact**: This information identifies the system, application or service owner
- **Application/Device Name:** This information provides the common name used as reference
- **URL:** If this system, application or service can be accessed by way or a uniform resource locator (URL), it will be captured as part of the inventory process.
- **Network Service:** This information identifies the inventoried item as one of the following service types:
    - Client
    - Content Management
    - Custom Application
    - Data
    - Database
    - Firewall
    - Internet
    - Operational Support
    - Report
    - Switch
    - Web
- **Public or Internal Client Application:** This information identifies the item inventoried item as public or internally-facing.
- **Capability:** This information identifies the inventoried item as IPv4, IPv6 or Dual-Stacked capable.
- **Inventory Completion Date (Planned and Actual):** This information is used for inventory purposes to determine when the item completed the inventory process at the Department.
- **Requirements Definition Completion Date (Planned and Actual):** This information identifies when the inventoried item will complete the requirements definition needed to move to IPv6, if necessary.
- **Design & Construction Completion Date (Planned and Actual):** This information will help in determining when the design and construction for moving the inventoried item to be IPv6 capable is planned and actually completed.
- **Testing Completion Date (Planned and Actual):** This date indicates when IPv6 testing will be completed for the inventoried item.
- **Implementation Completion Date (Planned and Actual):** This date indicates when IPv6 transition will be completed for the inventoried item.
- **Retirement Date (Planned and Actual):** This date indicates when the inventoried item will be retired. This date could be key

This information above will be used to in determine whether applications, systems or services will be required to transition to an IPv4/IPv6 dual-stack environment, remain IPv4 until retirement or retire prior to the IPv6 transition deadline. All department applications, systems and services will be placed into one of the following IPv6 deployment categories.

Retiring	The system will be retired before the IPv6 deployment deadline for external systems 9/30/2012 or Internal systems 9/30/2014
Legacy	This internal system will stay on IPv4 until the end of its lifecycle
Upgrade	The system will be upgraded to support dual stack IPv4/IPv6 by the transition deadline

4. Transition Strategy

The implementation of IPv6 will take place in the context of the Department's IT Governance process and impact the entire IT Portfolio at the Department. The following diagram describes how the IPv6 Transition Lifecycle will operate and impact various Department activities and organizations.



The Department's IPv6 Transition plan describes in detail the activities, milestones and deliverables that are produced by the various components of the organization as we execute the deployment of IPv6.

4.1. Management and Assignment of Resources

Enterprise Architecture Program Office guides the IPv6 Working Group. ED's Chief Enterprise Architect chairs the Working Group. The IPv6 Working Group consists of the PO IT Coordinators and major system representatives (G5, EDFACTS, MSIX, FSA). The group will also contain representatives from the Information Technology Services (ITS) and Information Assurance (IA) offices.

The tactical goals of the IPv6 Working Group meeting are to:

- Keep the management staff and system owners in the PO's informed and engaged in the IPv6 deployment
- Make decisions from a prepared agenda

- Consider information for decisions at the next meeting of the working group

The focus of the IPv6 Working Group is to ensure successful deployment of IPv6:

- Monitoring their office's IPv6 deployment activities and ensure they are completed on time
- Reporting their office's IPv6 deployment progress to the agency IPv6 Transition Manager
- Informing their office's about IPv6 issues, activities, and solutions across the agency
- Providing feedback to the IPv6 Transition Manager
- Identifying and managing the enterprise risks during the IPv6 deployment

The IPv6 Working Group monitors progress with updates from owners on the following activities:

- Overall transition (via performance measurement)
- Security
- Application Inventory
- IT Infrastructure
- Governance

The IPv6 Working Group guides awareness of IPv6 issues, activities, and solutions across the agency by:

- Updating the managers and system owners in the PO's on IPv6 deployment progress
- Reporting status across ED

4.2. Identifying Transition Candidates

The IPv6 Working Group will solicit input from system and application owners to identify common deployment and operational issues with the IPv4/IPv6 Internet and aid in determining solutions or workarounds to those issues. The IPv6 Working Group will also support the dissemination of information that identifies potential security risks and mitigates those risks. This work will be done in close cooperation with Information Assurance Services.

The IPv6 Working Group does not specify:

- Applications
- Transport Protocols
- Routing Protocols
- DNS
- Sub-IP Protocols

These items are the primary responsibility of OCIO-ITS. The IPv6 Working Group may provide input to OCIO, as needed, and cooperate with OCIO in reviewing solutions to IPv6 operational and deployment issues.

4.3. Technical Strategy during Transition

The transition to IPv6 will affect a broad spectrum of the Department's IT and network infrastructure, including routers, switches, servers and desktop computers, phones and other network infrastructure components. The transition will also affect network services such as Domain Name Servers (DNS), e-mail, network security and information assurance devices (firewalls, for example). It will affect operating systems, directory services administration, applications and related IT services.

The introduction of IPv6 capability will not significantly change the basic architecture of the Department's existing network (known as EDUCATE). Integrating IPv6 functionality and capability while continuing to support the Department's legacy IPv4 infrastructure (including IPv4-based applications) will be a significant challenge.

4.3.1. IPv6 Transition Method

The Department has determined that deployment of a simultaneous implementation of IPv4 and IPv6 network architecture (dual-stack) provides the best path to a successful IPv6 implementation with the least risk of disruption to the agency's networks, systems and processes. A dual-stack network architecture is one in which network hosts, routers, and switches support separate and distinct layers—one for IPv4 traffic and another for IPv6 traffic. The advantages of dual-stack architecture include:

- No additional overhead to manage tunnels or translation boxes;
- The ability to manage IPv6 and IPv4 traffic consistently;
- The ability to protect against potential security vulnerabilities associated with other transition mechanisms (especially tunneling, and tunnel broker mechanisms), and
- The ability to support the public, business partners, and other Government agencies utilizing either native IPv4 or native IPv6 according to their individual needs and requirements.

Establishing and maintaining dual-stack IPv4/IPv6 network architectures presents some technical challenges that do not override the substantial advantages of the dual-stack network architecture.

The Department's IPv6 transition strategy will integrate IPv6 capability with the Department's existing IPv4-based network in a structured and staged manner. The sequence of the Department's IPv6 implementation will proceed from the network core to the network edge. Utilizing the Department's existing technology refresh plans, IPv4-based routers and switches (and their associated subnets) will be made dual-stack capable; i.e., able to support either IPv4 or IPv6 communications. Alternate transition mechanisms will not be deployed. The Department has no plans to establish a pure or "native" IPv6 network for the foreseeable

future, but will establish and maintain a dual-stack IPv4/IPv6 capability throughout its network and systems.

4.4. Security Requirements during Transition

The Department must evolve its IT security policies and architectures to take into account new capabilities that will be required within IPv6. This evolution will help the Department take advantage of some of the inherent security-related features available within IPv6. Implementing IPv6 within an IPv4 network effectively creates a dual network layer, which inherently increases exposure to attacks. While many attack strategies for IPv6 may mimic known IPv4 attacks – such as sniffing, man-in-the-middle, flooding, application layer attacks and rogue devices – new forms of attack are likely. For example, many IPv4/IPv6 dual-stack technologies utilize tunneling which requires deeper packet inspection capabilities to scan tunneled packet information. Because production network experience with IPv6 and its resilience to attack is currently limited, proactive steps are necessary to minimize exposure. Security monitoring tools, perimeter gateway systems, remediation systems, processes and infrastructure and host security measures need to be tested and qualified in terms of IPv6 protocol support, attack detection and remediation capabilities.

Network security personnel should be trained on IPv6 protocol operation, including its security benefits and 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.

The OCIO Information Assurance Service will develop the IPv6 Security policy for using IPv6 on agency networks and systems, IPv6 device configuration standards, and continuous monitoring procedures. Several security implications of adopting IPv6 within an agency are provided below as initial guidance to identify a network security infrastructure plan within each agency.

- Security applications infrastructure currently used on an IPv4 network will need to be replicated, with an expectation that the same level of assurance is provided in the IPv6 network. Examples of those applications are Intrusion Detection, Firewalls, Network Management of IP Packets, Virus Detection, Intrusion Prevention, Secure Web Services Functions, etc.
- If end-to-end IPsec security is to be implemented, there will be a need to identify PKI, key management, and policy management infrastructures that meet the scalability and security verification requirements for intra-network communications (e.g. nodes, devices, and sensors).
- If end-to-end IPsec security is implemented, the current network perimeter security infrastructure applications (e.g., firewalls, intrusion detection systems) that depend on accessing and viewing IP transport data payloads must be aware that they will not be able to view that part of the IP packet and alternate mechanisms should be deployed.
- If VPN tunnels are used to encapsulate IPv4 within IPv6, or IPv6 within IPv4 as a transition method for deployment:

  - The tunnel endpoints between the VPN should be secured as the traffic transits the VPN.
  - When an encapsulated IPv6 packet enters or leaves the VPN and Intrusion Detection is required, it should be understood that the Intrusion Detection application or other network security method used to permit a packet on that network, has been ported to IPv6, as previously identified.
- Wireless network access from IPv6 nodes require in depth security analysis for implementation when stateless auto-configuration is used, in addition to current methods to secure IPv4 wireless networks.
- Seamless Mobility with IPv6 will need to support the required security as identified by the agency to permit secure access to the network whether across the internal network, or remote from an external network.
- IPv6 on a network should not be turned on by default unless all network security infrastructures are implemented. (Note that some products may have IPv6 enabled out-of-the-box.)

With the current upgrading of agencies' technical environments, many products have IPv6 capabilities already. It is anticipated many new threats and vulnerabilities will arise as attackers devote more attention to IPv6. As such, careful planning and additional attention to operating in a dual environment will be needed to deal with potential new threats and must be addressed by the agencies accordingly. IPv6 can be implemented securely on a network, but the guidance above is important to do it in the most secure manner possible.

4.5. Use of IPv6 Standards and Products

IT Governance requires consideration of NIST SP 500-267 *A Profile for IPv6 in the U.S. Government – Version 1.0*. The main purpose of this document is to identify and organize the vast collection of IPv6 specifications into subsets of mandatory and conditional requirements that may be of common utility in planning for and acquiring specific IPv6 products and services. The profile is primarily targeted to users in the following groups, shown in the following table:

Target Users for NIST SP 500-267A Profile

Group	Summary of Use
Testing and Accreditation Organizations	In Section 7, this profile outlines the plan for testing and documenting compliance to the specified requirements. The USGv6 test program will rely upon accredited laboratories executing standardized test procedures and methods. This profile provides the target, and thus starting point, for the further definition of the test program. As such, the profile will be of direct interest to test laboratories, accreditation bodies, and test equipment/systems vendors.
Developers	Developers of Host, Routers and Network Protection Devices and software should view this document as a statement of direction and intent for the USG IT networking marketplace. As such, the IPv6 technical requirements contained within the profile are expected to be implemented by significant numbers of this community.
Designers / Integrators	The engineers and managers responsible for systems development within the USG should look to this document as a strategic guide as to the networking capabilities to be expected in future networked systems. As such, they should consider how to use these capabilities in their broader systems-level designs, and should review these capabilities for gaps considered crucial to future systems requirements.

4.6. Costs Not Covered by Technology Refresh

A large portion of the IPv6 transition cost should be integrated into the normal product lifecycle replacement (refresh cycles). PO's should continue to include IPv6 capabilities into the planned product procurements of their existing information technology budgets. IPv6 remediation costs that are not covered by the normal technology refresh process must be planned and budgeted using the Capital Planning and Investment Control Process. Examples of costs that may not be addressed by the technology refresh process are IPv4 dependency assessment and system testing facilities and services. By including system upgrades to IPv6 as part of their regular procurement process and budget planning for related cost PO's can take an evolutionary approach towards adoption of the new protocol.

5. Transition Governance

This section describes the federal policy and guidance, roles and responsibilities, governance structure, performance measurement and reporting expectations for IPv6 activities at the Department.

5.1. Policy

Along with this document, the following Federal policy and guidance has been issued, governing the transition planning process for IPv6 in the Federal government.

Document Title	Document Number/Date	Organization
Transition to IPv6 Memorandum	Sept 28, 2010	Vivek Kundra, Federal CIO
Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government	May 2009	The Federal CIO Council Architecture and Infrastructure Committee, Technology Infrastructure Subcommittee, Federal IPv6 Working Group
NIST Profile for IPv6 in the U.S. Government – Version 1.0	NIST SP 500-267A	National Institute of Standards and Technology (NIST)
Federal Acquisition Regulation	(FAR) 11.002(g)	General Services Administration (GSA)
An Internet Transition Plan	RFC-5211	(Internet Engineering Task Force) IETF

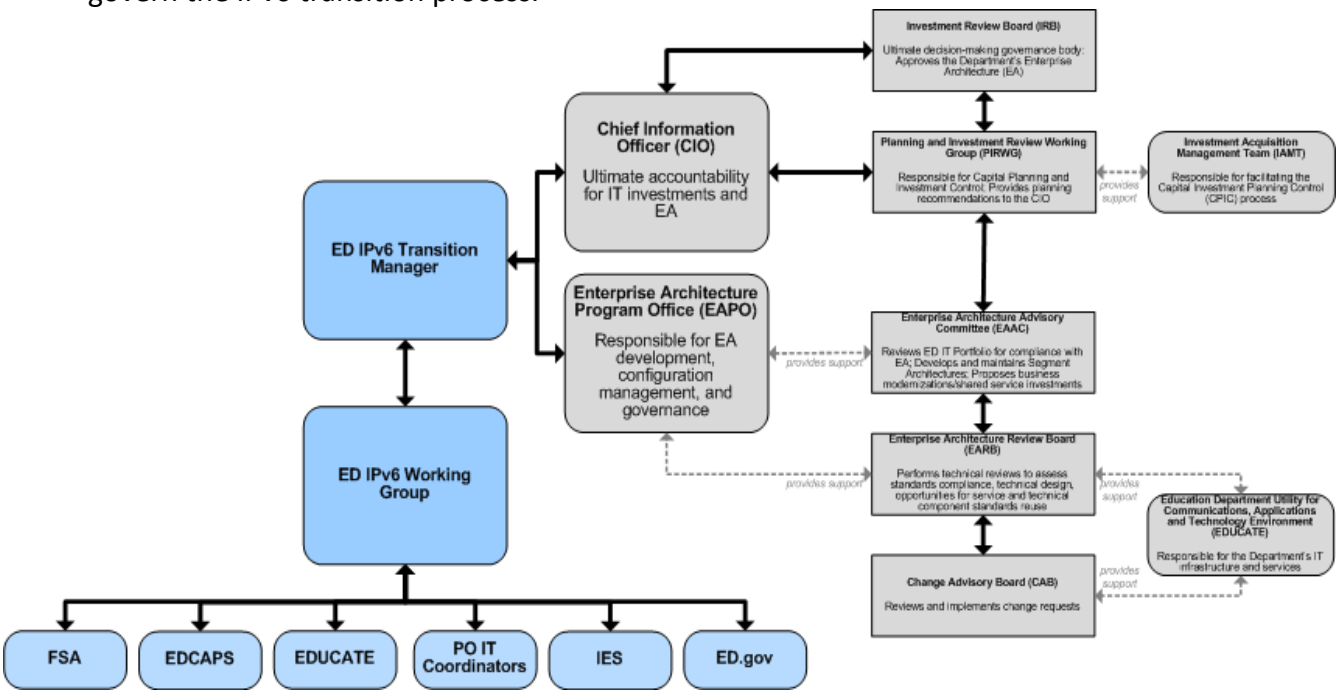
5.2. Roles and responsibilities

The following groups have assigned activities and milestones as part of the Department's IPv6 transition strategy or monitor these activities for the Department.

Group	Group Description
Application Owners	Application Owners are project managers of the Department's software system investments.
Enterprise Architecture Program Office	The Enterprise Architecture Program Office ensures that financial decisions for acquiring technology are driven by business needs.
Information Assurance Services (IAS)	Information Assurance Services (IAS) manages the Department's information technology security program and ensures the confidentiality/privacy, integrity, and availability of the Department's information and information resources.
Contracts and Acquisitions Management (CAM)	Contracts and Acquisitions Management (CAM) is responsible for the solicitation, award, administration, and closeout of all contracts and other acquisition instruments for the Department.
IPv6 Working Group	The purpose of the Working Group is to coordinate the transition efforts at the Department level
Information Technology Services (ITS)	Information Technology Services (ITS) is provides information technology oversight and operational support including oversight of infrastructure, purchase of IT hardware, software and other related items.

5.3. Management structure

The following diagram illustrates the management structure the Department has put in place to govern the IPv6 transition process.



5.4. Performance measurement

As noted in the management structure, the Department's EA Program Office (EAPO) will lead the IPv6 transition by coordinating the execution and reporting of the agency's IPv6 deployment activities . The EAPO will use the milestone planned dates versus actual dates in the IPv6 Transition Activities and Milestone Planning table in this document to measure transition status and performance.

5.5. Reporting

Each system and application owner will report the certification status of IPv6 interoperability, information assurance, and functionality requirements. The content will include schedule and risk issues. These reports will be read by:

- The Office of Management and Budget
- The Office of the Chief Information Officer
- Planning & Investment Review Working Group (PIRWG)
- Enterprise Architecture Advisory Council (EAAC)
- ED Senior Managers
- ED System and Application Owners

6. Acquisition and procurement

In accordance with *Federal Acquisition Regulation (FAR) 11.002(g),* the Department needs to include relevant standards for IPv6 in all IT related acquisitions that have any relation to the network. Adding IPv6 support to new procurement beyond the core network helps enterprises meet the internal adoption deadlines for transition to IPv6.

Additionally, agencies must review NIST SP 500-267A *Profile for IPv6 in the U.S. Government – Version 1.0* to specify future IPv6 product acquisitions. In summary, ED should consider:

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

The Department recommends the following language be used in all IT related acquisition and procurement documents that have any relation to the network:

> **Internet Protocol version 6 (IPv6)**
>
> The Contract shall provide COTS solutions that are IPv6 capable. An IPv6 capable system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific criteria to be deemed IPv6 capable are:
>
> An IPv6 Capable system must meet the IPv6 base requirements defined by the USGv6 Profile and Testing program as found here "http://w3.antd.nist.gov/usgv6/testing.html".
>
> Systems being developed, procured or acquired shall maintain interoperability with IPv4 systems/capabilities.
> Systems shall implement IPv4/IPv6dual-stack and shall also be built to determine which protocol layer to use depending on the destination host it is attempting to communicate with or establish a socket with.
> If either protocol is possible, systems shall employ IPv6.
>
> The contractor shall provide IPv6 technical support for system development, implementation and management.

7. Training

There are a number of factors that will affect the success and duration of the transition process. At the top of that list of factors are: adequate planning, a well developed IT strategy, and training. IPv6, while built on many of the fundamental principles of IPv4, is different enough that most IT personnel will require formalized training. The level of training required will vary and depend upon the role a member of the organization's IT staff plays in developing, deploying, and supporting IPv6 integration. For the purposes of clarification, four main categories of education are specified:

Awareness – This is generalized information about IPv6 and IPv6-related issues. This type of education is most commonly found via workshops, seminars, conferences, and summits. These types of events typically provide an overview of IPv6 technologies, identify vendors that support IPv6, and provide participants with a rudimentary understanding of the IPv6 technology, as well as business drivers, deployment issues, and potential services/products enabled by IPv6.

Architectural – Training in this category should be very detailed and oriented towards those individuals who will have primary responsibilities in architecting and deploying IPv6 (those identified in Application, Infrastructure and Governance groups in the activities and milestones table of this document). Although the type of subject matter will be quite broad, particular attention should be paid to the fundamentals of IPv6, DNS and DHCPv6, auto-configuration, IPv6 address allocation, transition mechanism, security principles for IPv6 environments, and mobility. Additional topics covered should be routing, multicasting, and principles for connecting to the IPv6 Internet. These topics are the areas where participants will encounter the greatest number of new subjects (relative to IPv4), and will have the greatest impact on the development of successful integration plans.

Operational – Once IPv6 has been integrated into the network, it will need to be supported. Operational training will consist mostly of job specific education targeted to a participant's job responsibilities. Core topics such as the fundamentals of IPv6, auto-configuration, and transition mechanisms will undoubtedly be covered. However, the bulk of operational training should focus on supporting applications or protocols that have IPv6 underneath them. One example is training for system administrators focusing on supporting IPv6-enabled e-mail and web servers. Operational training will often be hardware or software specific, generally produced by, or for, a particular vendor product.

Specialized – As IPv6 deployment advances and the base level of understanding become more pervasive, the need for specialized training will emerge. This type of training should focus less on IPv6 specifically and address greater technological topics where IPv6 plays an important role. An excellent example would be the area of Mobility. Projects such as MetroNet6 (http://www.cav6tf.org/html/metronet6.html), focus on utilizing IPv6 and Mobility concepts for

improved communication systems for first responders. Course work in this area would cover not only Mobile IPv6, but also topics such as MANET, NEMO, mobility-specific security issues, access media, and possibly low bandwidth compression algorithms.

This plan recommends that as part of the inventory and assessment phases of the transition activities that the Application, Infrastructure and Governance groups identify the necessary training mechanisms for their groups and account for them in their individual planning activities. In addition, the Federal CIO Council AIC IPv6 Working Group will work in conjunction with the Department, other agencies, industry, and OMB to identify specific agency training needs and potential solutions.

8. Testing

The IPv6 Working Group will be able to review progress toward implementation with aid from test results. As discussed below in section 4.2.5.1, *IPv6 Test Program*, the test strategy discussed in this document includes general purpose IPv6 device test that is appropriate for all Agencies. Agency specific deployment and acceptance testing guidance is provided in the section 4.2.5.2, *Establish an IPv6 Test Lab*. Application-oriented considerations are discussed in the section 4.2.5.3, *Planning for Application Transition*.

8.1. IPv6 Test Program

NIST has established a test program based on International Standards Organization (ISO) 17025 accredited test laboratories and standard reference tests, to assure compliance of Hosts, Routers and Network Protection Devices. The NIST SP 500-273 document provides guidance on IPv6 test methods and validation. The goal of the test program is to have IPv6-compliant devices available for acquisition by July 2010.

8.2. Establish an IPv6 Test Lab

NIST SP 500-273 recommends setting up a test lab for the safe, controlled introduction of new technology into your network and prototyping with an emphasis on small scale validation of targeted performance outcomes (e.g. Experimentation with secure IPv6-enabled teleworking.) Testing in a lab enables the agency IT group to perform tests that could potentially be disruptive or introduce a security risk if deployed on the production network. **Application, System,** and **Infrastructure** owners should identify their respective test lab to the IPv6 Working group.

All networked applications, including clients and servers need to be modified or redesigned to function in an IPv6 networking environment. Application owners should test explicitly for these modifications.

Initially, applications will be required to perform common IPv6 functions and will need to evolve to incorporate more advanced features of the protocol. The test planning for IPv6 application transition should include:

- Accounting for all inventoried applications
    - Agency Government-off-the-shelf (GOTS) applications
    - Commercial-off-the-shelf (COTS) applications
    - Existing Application upgrades and refresh
    - New application developments and procurements
    - Applications at end-of-life
- Legacy operating systems and applications according to inclusion in the transition or targeted for retirement during an appropriate technology refresh period.
- Testing milestones

- Accounting for application interoperability. There may be a need to transition and release enterprise applications in blocks for interoperability purposes.
- COTS application transition schedules: Work with vendors to get realistic transition and availability schedules so you test the actual version to be released.