DEPARTMENT OF VETERANS AFFAIRS

ENTERPRISE TRANSITION PLAN
FY 2010 – FY 2014

Prepared by the

Office of Enterprise Architecture and Innovation (005E1)

Pre-Decisional Draft, May 2009

APPENDIX D.4.1 IPv6 Initiative Status

A proposal for funding the implementation of IPv6 in VA was presented to the VA ITLB in April/May 2009. The following information was included in the proposal.

Investment Start Date: 1/1/2011
Expected Deployment Date: 12/31/2014
OI&T PM: Steven Pirzchalski
Business Sponsor: OI&T
Category: Proposed Investment
Description:

The Office of Management and Budget (OMB) mandated that all federal agencies move toward utilizing Internet Protocol version 6 (IPv6) on their production networks. VA successfully met the original June 2008 OMB mandate and was acknowledged as a Level 1 agency within the federal government. In addition to being an OMB mandate, IPv6 is a foundational element of many of VA's future technologies. IPv6 will improve VA's network services and telehealth programs through the use of new features such as addressing, network management, and enhanced security. In addition, Enterprise Architecture (EA) Framework 3.0 requires that IPv6 be part of future technology initiatives; therefore, IPv6 will replace IPv4 as the standard IP protocol by 2013. The IPv6 team is currently beginning Phase II activities as requested by the Federal Chief Information Officer (CIO) Council. IPv6 is aligned with the move to veteran-centric services. It represents the next-generation network (NGN) protocol that will drive the development of or enhancements to future applications for mobility and security that will greatly benefit rural veterans as well as those in metropolitan areas.

IPv6 flexibility and other capabilities will allow VA to expand telehealth and benefits services to veterans and their families. The improved security of IPv6 directly benefits veterans by protecting their personal information as they connect to VA through their home Internet accounts or through business partner accounts (i.e., other medical organizations or devices that use IPv6). This increased security will allow veterans to feel more comfortable about transmitting their personal information electronically and confident about VA's ability to protect their personal data. In addition, IPv6 auto-configuration and remote management capabilities make it easier for veterans to use home health devices that are IPv6- enabled. IPv6 also allows VA to reach more patients and extend services to veterans in rural locations, ensuring that they receive the same level of care as veterans who live closer to VA medical centers (VAMCs). Finally, IPv6 more efficiently supports mobile communications, allowing VA to better serve veterans through more effective monitoring and home health care programs.

IPv6 will allow VA to "flatten" the existing network and significantly reduce the number of intermediate routing devices. This change reduces cost and complexity while improving performance, manageability, and maintainability. IPv6 provides enhanced security features that will allow VA to implement a core security architecture that will improve its compliance with Federal Information Security Management Act (FISMA) and Health Insurance Portability Accountability Act (HIPAA) regulations, while enabling faster and secure deployment of new

programs. OMB and the Federal CIO Council are projecting that business cases will be developed for IPv6 as early as February 2009, and implementation should begin in FY 2011 and beyond. IPv6 is connected to other major initiatives such as Trusted Internet Connection (TIC), Networx Transition, Homeland Security Presidential Directive 12 (HSPD-12), IT Infrastructure Line of Business, and Federal Desktop Core Configuration (FDCC).

Transition Status:

In August 2005, OMB issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)" mandating that all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure by June 2008. The memo stated that each agency must take initial actions as follows, which have been completed and submitted to OMB for VA.

November 15, 2005	• Assign an official to lead and coordinate agency planning. • Complete an inventory of existing routers, switches, and hardware firewalls (see Attachment A for details). • Begin an inventory of all other existing IP compliant devices and technologies not captured in the first inventory. • Begin impact analysis to determine fiscal and operational impacts and risks of migrating to IPv6.
February 2006	• Using the guidance issued by Chief Information Officers Council (CIO Council) Architecture and Infrastructure Committee, address each of the elements in Attachment C in your agency's IPv6 transition plan and provide the completed IPv6 transition plan as part of the agency's Enterprise Architecture (EA) submission to OMB. Additional guidance on your agency's EA submission will be forthcoming. • Provide a progress report on the inventory and impact analysis, as part of the agency's Office of Enterprise Architecture Management (OEAM) submission to OMB.
June 30, 2006	• Complete inventory of existing IP compliant devices and technologies not captured in first inventory. • Complete impact analysis of fiscal and operational impacts and risks.
June 30, 2008	• All agency infrastructures (network backbones) must demonstrate that it can use IPv6 and agency networks must be able to interface with this infrastructure. Agencies will include progress reports on meeting this target date as part of their EA transition strategy *[R2]*.

Although subsequent guidance softened this requirement, in initial planning, VA's IPv6 working groups committed to and established a goal of March 2008 to meet the deadline. VA met the goal and proved its compliance on March 17, 2008, allowing the additional calendar time to execute bonus multi-agency testing. Additionally, VA has plans to:

- Conduct a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements.
- Develop a sequencing plan for IPv6 implementation, integrated with agency Enterprise Architecture.
- Develop IPv6-related policies and enforcement mechanisms.
- Develop training material for stakeholders.
- Develop and implement a test plan for IPv6 compatibility/interoperability.
- Deploy IPv6 using a phased approach.
- Maintain and monitor networks.
- Update IPv6 requirements and target architecture on an ongoing basis.

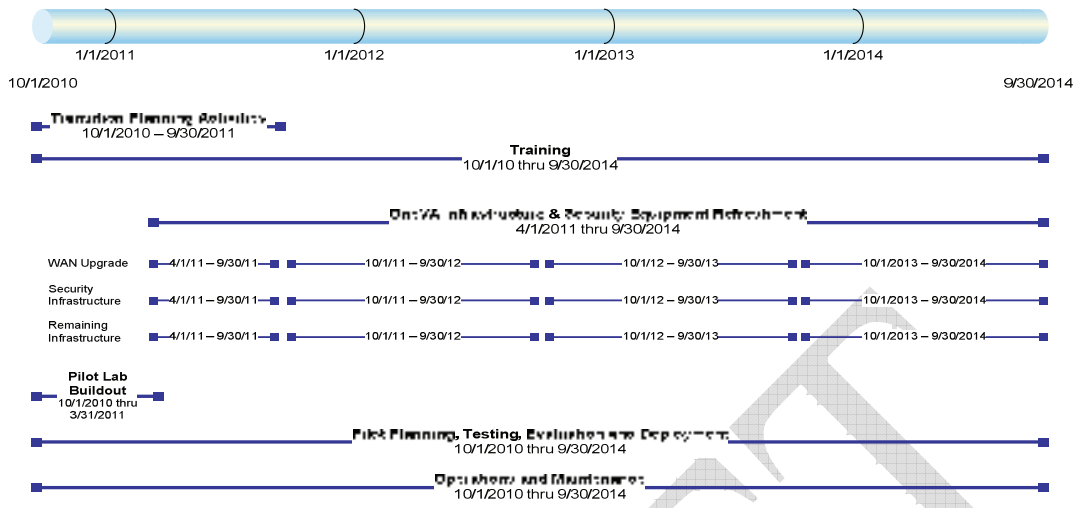
Transition Schedule:

VA transition working groups have recommended that VA backbone be ready to operate with IPv6 capability by October 2011. VA's planning is based upon this recommendation since the October 2011 date will provide a time period for finding resolutions to any problems encountered. The consensus among VA network development and management officials is that operating VA backbone with IPv6 capability is feasible between FY 2011-14.

It will also be necessary, however, to have security and network management products available and operational that can ensure the proper operation of the backbone within relevant standards and requirements.

VA has chosen to use a 'dual stack' approach to implement IPv6 on the network backbone. Dual stack is strongly recommended by the Transition Working Group as the preferred IPv6 deployment approach. In a dual stack environment IPv4 and IPv6 protocols coexist and are supported by OSI level 3 devices such as routers. This configuration will allow the transition to IPv6 by early adopters while continuing to support the existing business functions using IPv4.

VA's IPv6 Transition Schedule identified various aspects depicted at a high level. The Transition working group approved and forwarded the original master schedule plan to VA's Steering Committee, which is responsible for tasks and resources involved in the project. The original plan is the basis of the Time Line illustrated below.



The plan above, while not absolutely complete, starts well after the successful IPv6 network test which met OMB's mandate of June 2008. This Time Line shows the start of an aggressive IPv6 "proof of concept" Pilot Program and continuous activities to enable successful IPv6 deployment. These milestones will play a large part in the rapid implementation phase of the future. ***They are included in the VA Enterprise Transition Plan's Sequencing Plan.***

With careful coordination between all VA activities including VHA, VBA, NCA, and all other VA Programs, the infrastructures that support VA applications will be transitioned from IPv4 to IPv6. The actual transition will be a multi-phased process based on time and functionality. Transition mechanisms will be installed and enabled, program by program and site by site to provide a core suite of IPv6 functionality.

VA has yet to establish the goal of completing the transition to IPv6 for all VA infrastructure networks, although the initial OMB mandate was met as previously described. Successful transition must consider the diverse and evolving nature of VA internal networks. A successful transition will ensure the necessary IPv6 infrastructure is available, that transition issues are addressed, and that all VA applications will continue to work over IPv6 networks.

Transition Documentation:

The following documents are IPv6 artifacts available on the VA EA website:

- External Agency Internet Test Final
- Interagency IPv6 Test
- Interagency IPv6 Test 06-24-08
- VA IPv6 Test Results, Version 3
- VA Transition Plan for Internet Protocol Version 6 (IPv6), Version 3.00, March 25, 2009
- VA IPv6 Demonstration Plan Results V1.00, May 2008
- VA Internet Protocol Version 6 (IPv6), Impact Analysis, Fiscal and Operational Impacts and Risks, April 2009
- VA Internet Protocol Version 6 (IPv6), Pilot Process Document, Version 1.0, April 2009