United States

Department of Veterans Affairs

Internet Protocol version 6 (IPv6) Impact Analysis

Fiscal and Operational Impacts and Risks

April 2009

IPv6 Project Management Transition Office
Telecommunications Operations Management Service
Office of Information and Technology

Table of Contents

1 EXECUTIVE SUMMARY

The Department of Veterans Affairs (VA) Office of the Chief Information Officer (CIO) and the Office of Telecommunications, Office of Information and Technology (OI&T) continue to make progress with the IPv6 transition. VA's IPv6 Project Management Transition Office (PMTO) has assessed the impact of the IPv6 backbone network deployment on VA, its mission and its personnel to date. The risks outlined in this document are based on:

- Interviews with subject matter experts within VA
- Review of current literature and Federal guidelines
- Discussions with industry experts
- Information produced by VA's transition teams
- Results of the inventory of the components of VA's backbone infrastructure

This impact assessment will address a summary view of costs for the planned five year deployment estimating the planning, infrastructure acquisition, training, pilot test planning and execution as well as operations and maintenance. The assessment will also detail the risks associated with the transition from IPv4 to IPv6. This list of risks establishes a baseline VA will need to monitor as it progresses through the acquisition and installation of infrastructure, training, configuration and management. As with any long range plan, the assessment will need to be updated on an annual basis.

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.

Analysis of the risk areas expected during the transition shows that of the nineteen total areas of risk, seven present the greatest risk to VA during the transition to IPv6. Below is a list of those areas of greatest risk. For a description of how criticality was determined, see section ***Appendix A – Summary of Risk Criticality***.

- Reliability of Systems
- Dependencies and Interoperability Issues
- Surety (Asset Protection) Issues
- Security
- Project Resources
- Human Capital
- Technical Obsolescence

In conclusion, the IPv6 deployment on the network backbone presents both fiscal and programmatic impacts but the risks and the mitigation steps sited are reasonable. Certain hardware replacement and upgrade costs will be funded from the technology refresh budget. Other costs such as the establishment of a program office, planning for the transition, planning and execution of pilot tests, assessment of and testing of security issues, and communication and training of staff must be funded as additional costs not tied to VA's IT technology refresh. The detailed assessment of the risks involved in the IPv6 deployment has been conducted. In collaboration with stakeholders throughout VA, mitigation strategies have been identified for the risks detailed in this assessment

2 INTRODUCTION

2.1 IPv6 Background

The Internet Protocol (IP) is the network protocol on which today's Internet is based. It enables a variety of disparate networks, computers, and other devices to communicate with each other using a common protocol. Today, the Internet Protocol has matured and has established itself as the chief vehicle for electronic commerce and many other applications.

IPv4 has been in use for more than 30 years and is expected to continue to be in service for many more. However, the continuous growth of the global Internet requires that its architecture evolve to accommodate new trends in user applications and new technologies. In addition, a popular rationale for the adoption of IPv6 is the requirement for additional IP addresses.

There is a strong argument that countries or regions that move to gain early IPv6 adoption will have economic advantages. Consequently, for the United States, the main motivator is ensuring that the US networking environment remains competitive with the international community. Some nations, most notably Japan and the People's Republic of China, are rapidly deploying IPv6 networks. The United States must make the migration to IPv6 to be able to continue its technological parity internationally.

Beyond the federal mandate for IPv6, the motivation for the effort to deploy IPv6 is that an IPv6-based world is inevitable. While the precise date when address space for IPv4 will be depleted is subject to debate, there is arguably a point when such depletion will be the case. Therefore, it would be prudent to begin planning for IPv6 deployment in an orderly manner now and avoid accelerated expenditures and crash schedules in the future.

Although IPv4 currently supports many of today's applications, it has several shortcomings which complicate, and, in some cases, present a barrier to the further development of the Internet. IPv6 was designed to overcome these shortcomings and barriers. Features of IPv6 include:

- Elimination of the need for Network Address Translation (NAT). That elimination will
    a. Restore the original peer-to-peer intent of the internet
    b. Simplify network-layer encryption and authentication and
    c. Provide the potential for greater security by exposing and not hiding all IP addresses
- Auto-configuration of IPv6 hosts when connected to an IPv6 network (either wired or wireless)
- Built-in security with the IP framework vs add-on patching
- Embedded IPSec providing unified security strategy for the entire network
- Expanded use of different types of addresses
- Integrated QoS support

2.2 IPv6 and the OMB Mandate

The project to transition VA to IPv6 originated with the Office of Management and Budget (OMB) Memorandum for Chief Information Officers, M-05-22 which detailed the first phase of IPv6 Transition Planning needed. VA successfully met all of the OMB's initial requirements for determining IPv6 is capable of operating on the backbone before the June 2008 time frame.

Figure 1 below is a conceptual view of VA network depicting the separation of VA Backbone (Infrastructure) and the other layers that depend on connections with the backbone.

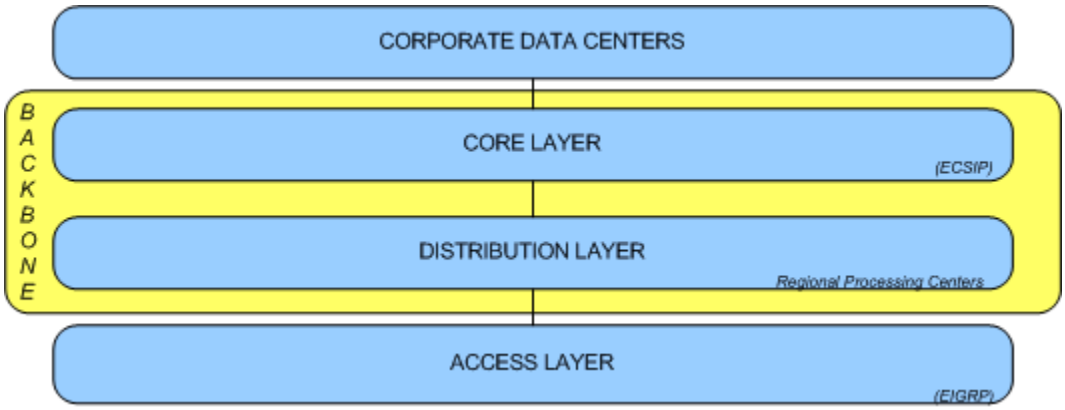


Figure 1 – Veterans Affairs Network Backbone

Additionally, milestones were distributed to all federal agencies, creating additional requirements to the original IPv6 mandate. There have been specific Desktop Security requirement for Microsoft Windows XP and Vista Operating Systems - Dates are specified below:

May 1, 2007

Agencies were to submit plans to OMB for deploying standard desktop configurations for Microsoft Windows XP and Vista. Submission should include plans for:

- Testing configurations in a nonproduction environment to identify adverse effects on a system's functionality.
- Implementing and automating enforcement of these configurations.
- Restricting administration of those configurations to authorized employees.
- Applying patches for XP and Vista vulnerabilities.
- Providing documentation of any deviations from these requirements and why they need to be different.
- Making sure that these standards are part of the agency's capital planning and investment control processes.

June 30, 2007

Agencies must ensure that new acquisitions support the standardized desktop configurations and require vendors to certify their products can work under those standards.

February 1, 2008

As an element of the Department of Veterans Affairs FY07 FISMA Report an annual update on security is now also due to OMB. VA IPv6 workgroups must submit specific IPv6 pertinent information, as well as implementation plans to VA Office of Cyber Security OCS and cc VA Enterprise Architecture Office; for inclusion of IPv6 into VA FY07 FISMA Report, along with an updated Risks Assessment and Document adhering to Best Practice guidance.

The Federal Desktop Core Configuration required that all Federal agencies standardize the configuration of approximately 300 settings on each of their Windows XP and Vista computers. VA complied with this mandate in the second quarter of 2008. In October 2008, NIST Special Publication 800-68 was created for Windows XP. This guide provides detailed information about the security features of Windows XP, security configuration guidelines for popular applications, and security configuration guidelines for the Windows XP operating system. VA has actively followed standards and guidelines set by NIST Special Publications.

2.3 IPv6 Deployment Strategy

To address the complete deployment of IPv6 on the backbone and to supporting infrastructure the IPv6 PMTO has devised a five year strategy. Several activities in the strategy run parallel throughout the five years to provide continued focus and mitigate risks. Training and Communication are constants throughout the strategy to insure the focus and technical knowledge of IPv6 are maintained. One of the key elements of the strategy to mitigate technical risks is by planning and executing various pilot tests both in a lab and in isolated network installations. The figure below is a timeline depicting the five year transition strategy for VA's implementation of IPv6.

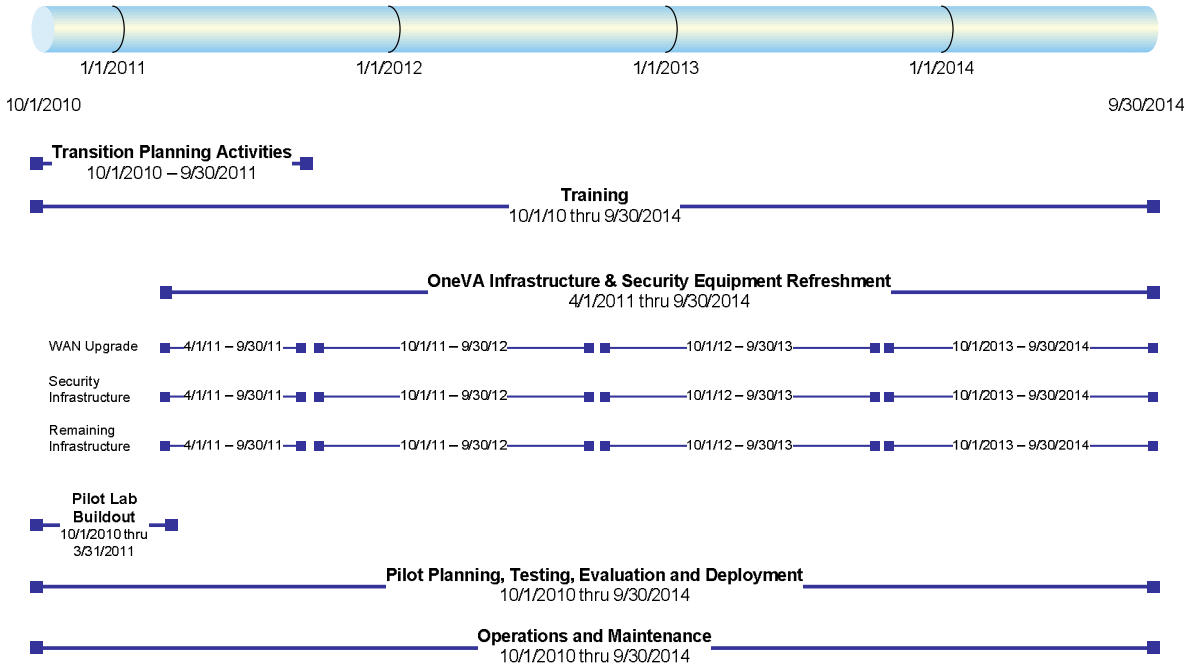


Figure 2 – Timeline - IPv6 Transition & Pilot Tactical Strategy

2.4 Purpose

This document describes risks and impact analysis for deploying IPv6

2.4.1 Scope of this Impact Analysis

The scope of this analysis identifies potential impacts to VA as they relate to cost or risk. The cost impacts are expressed as the high level estimated costs of the transition to IPv6. The risks are the project risks both technical and non-technical associated with making VA backbone IPv6-capable. Our reference of IPv6 capability is taken to mean that the backbone comprised of the core and the distribution layer can pass traffic using IPv6 addresses while meeting all requirements for security and operations. The capability must allow for the transmission of IPv6 traffic across the backbone between VA local area networks (LANs), to and from the Internet, and to and from another government agency.

2.4.2 Impact Analysis Approach

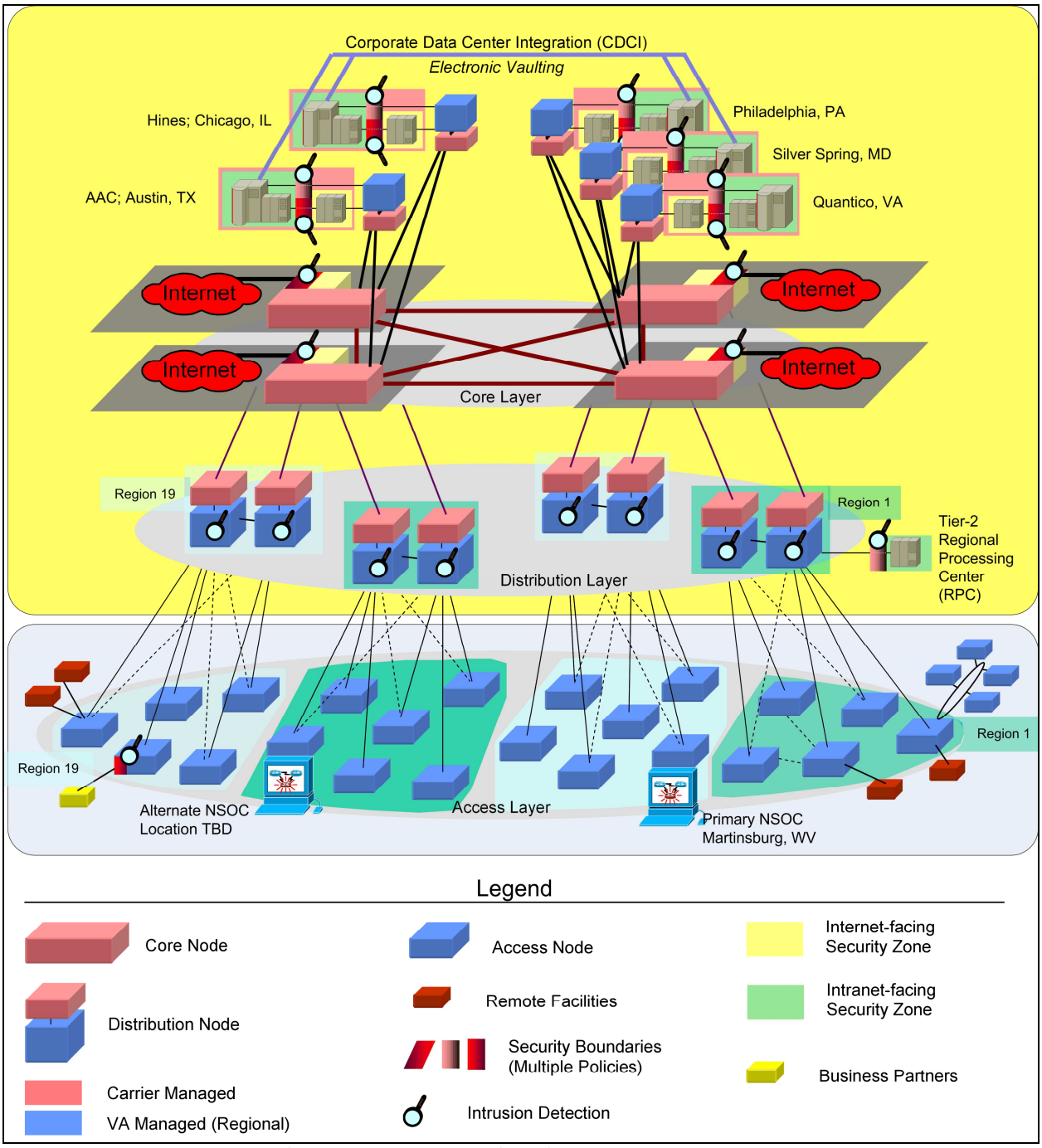
Organizations use risk analysis to determine the extent of potential problems with a project through its system development life cycle (SDLC). The result of this process helps to identify appropriate controls for reducing or eliminating the risk; this process is called risk mitigation. The methodology used in this document first establishes the boundaries of the system and then identifies the resources and the information that constitute the system. The following techniques were used to collect data:

- Questionnaires were developed to collect relevant information.
- On-site interviews were conducted with system support and management personnel.
- System documentation, policy documents, and security-related documentation were reviewed.
- A chart outlining the probability of a potential vulnerability and the magnitude of same was derived from information collected based on the OMB Exhibit 300.

2.4.3 System Characterization

From an enterprise perspective, the backbone spans the facilities, services, and network devices needed for the functioning of data communication among VA communities. For IPv6 planning purposes, the backbone spans all network components contained in the core and , distribution layers, as illustrated in ***Figure 3 – Veterans Affairs Network***. Corporate data centers connect via distribution nodes to the core layer. Connection to the external Internet is made via the secure enterprise internet gateways that operate in the core layer. All other VA connections, from Veterans Health Administration, Veterans Benefit Administration, and the National Cemetery Administration, are made via distribution nodes at the access layer. Distribution nodes consist of a pair of routers, one which is carrier managed and the other which is VA managed on a regional basis.

This definition of Distribution Layer is depicted in ***Figure 3 - Veterans Affairs Network*** (see following page). VA backbone items are highlighted in yellow and the remainder of VA network infrastructure is displayed in blue.



Note: Area in yellow depicts two of the nineteen regions and four of the six Data Centers

Figure 3 - Veterans Affairs Network

3 COST ESTIMATES

The cost estimates have been determined by the activities of the project. These estimates identify those cost factors responsible for the incremental costs of deploying IPv6 on the network backbone. VA intends to transition to IPv6 principally by upgrading equipment and software as part of the normal technology refreshment process. IPv6 capabilities will be added until such time as IPv6 service can be supported across the backbone. Additionally, there will be services and equipment "above and beyond" normal technology refresh that VA will need to fund as "costs" associated with the management and implementation of the transition of the backbone to IPv6.

Table 1 below provides a high level view of the estimated costs associated with the planning and deployment of IPv6 from 2009 through to 2014.

Strategy Phase	Cost
Transition Planning	$ 7,000,000
OneVA Infrastructure and Security Equipment Refreshment	$ 100,000,000
Training	$ 7,500,000
Pilot Lab Build out	$ 1,000,000
Pilot Planning, Testing, Evaluation and Deployment	$12,300,000
Operations and Maintenance	$7,150,000
TOTAL ESTIMATED COSTS	$ 134,950,000

Table 1 – IPv6 Transition Strategy-Cost Estimates

See ***Appendix B – Cost Details*** for a FY year breakdown of the high level costs.

3.1 Transition Planning

Detailed IPv6 transition planning will create the roadmap for VA's transition from IPv4 to IPv6. As part of the transition planning process, the following activities and work products will be produced:

- Transition Plan
- Communications Plan
- Inventory Assessment
- Training Schedule
- Network Assessment
- IP Address Management Tool Evaluation and Selection
- Application Assessment
- Conference Planning
- Integrated Project Schedule

For a Fiscal year breakdown of Transition costs see ***Appendix B – Cost Details***

3.2 OneVA Infrastructure & Security Equipment Refreshment

The planning as well as infrastructure and security refreshment needed to complete the transition to IPv6 will span five years ending in September, 2014. Prior to the start of the transition, the PMTO will be planning transition activities and testing to insure the correct transition is made. During the four year refresh period that follows, the IPv6 PMTO will be managing the transition to a dual stacked IPv4/IPv6 based infrastructure for VA WANs, Security Infrastructure, and Network management tools. The dual stacked solution allows VA to take advantage of opportunities with IPv6 capabilities when they are available while continuing to support the IPv4 population and transition over time.

The infrastructure equipment involved in the refresh will sustain the devices supporting the WAN, security infrastructure and remaining infrastructure. There were no shareware devices, client devices or devices identified as "COTS modified by government contract but still available to public" in VA backbone network. While there were authentication devices and freeware devices, none were identified as non IPv6-compliant. There are instances were a manufacturer has not provided an upgrade plan or technical refresh date for a device, particularly if the device is already IPv6-compliant and the device has not reached an end-of-life designation.

Some of the devices listed below will be replaced as part of technology refresh. However, there may be many cases where devices identified as *end-of-life* or *legacy* serve acceptable roles in supporting IPv4 traffic and these devices would be retained in order to continue supporting IPv4 traffic over the course of the five year transition plan.

FIGURE 4 : Network Equipment Type vs. Function vs. IPv6-Capable Status (color coded)

Device Type	Series / Model	Model	Model	Model	Model	Model	IPv6 capable?
Router	**2500**	2503	2505	2520			No
	2600	2620	2621	2621xm	2651xm		Yes
	2800	2801	2811	2821			Yes
	3600	3620	3640	3662			Yes
	3700	3725	3745				Yes
	3800	3825	3845				Yes
	4000	4700					No
	7200	7204	7206				Yes
	7500	7505	7507	7513			Yes
	7600	7609					Yes
	curm2fe						No
Switch	**Cat2900**	2926	2950				No/Yes
	Cat3500	3550					Yes
	Cat3700	3750					Yes

Device Type	Series / Model	Model	Model	Model	Model	Model	IPv6 capable?
	Cat4000	4006					Yes
	Cat5000	5302					Yes
	cat6000	6509	6513				Yes
VPN Server	ASA5540	C2651XM	C3745				Yes
Firewall	ASA5540	CSM	PIX535	Dell2850	Trafficshield		Yes/No
Proxy/Cache	CyberGuard WW1000	IronPort C600	Cisco CE-7305	NetApp NetCache C3300			Yes/No
Unknown (sensitive)	Enterasys DSNSA-GE200-SX	Manhunt SR1200	Proventia G1200, G400	ISS RealSecure IP0380	SourceFire LX50	SourceFire Unknown	No

Legend:

Black Object: IPv6-Capable
Red Object: IPv4-capable only
Yellow Object: IPv6-capable status unknown

CSM: Firewall Switch Module (Cisco)
Cisco CE-7305 : "Content Engine" / Web cache
NetApp NetCache C3300 : Web cache
CyberGuard WW1000 : "Content Security Appliance" (web proxy)
IronPort C600 : Web proxy

3.3 Training

VA Training Department, in conjunction with representatives from organizations within VA, identified a number of stakeholder groups and audiences that will require differing levels of training. The training is crucial to the successful transition to IPv6 and subsequently provides support and maintenance. Material for training was developed to target the following three population audiences:

Training Material	Audience
Architectural	Enterprise Architects
	Network Managers
	Technical Managers
	Telecom Managers
	Security Managers
Operational	Network Engineers
	Network Specialists
	System Developers
	Telecom Specialists
	Support Personnel
General Population	Management
	Executives

Train-The-Trainer sessions have been conducted in both Salt Lake City and Herndon for the Architecture and Operational communities. Also for the General audience, several distributions via intranet posting, pamphlets, and an informational video have been produced. However, as VA infrastructure transition becomes more widespread and the availability of IPv6 becomes more prevalent, training in all three population types will be needed over the course of the next five years.

The training department provided cost factors and estimates. The following contributors to the cost estimates were identified as:

- Travel
- Facilities – In-house or contractor provided facilities
- Trainer – In house or contractor
- Training Materials - In house or contractor provided

A Fiscal Year breakdown of training costs are found in ***Appendix B – Cost Details***

3.4 Pilot Planning and Execution

To mitigate the risks that are identified in this plan, testing of the IPv6 deployment will be extremely important. To that end, the Transition team strategy will be to establish a pilot testing lab to install various IPv6 devices and to test them with IPv6. The lab will also be used to conduct pilots throughout the transition. The pilot lab will allow for technology destined to be within VA WAN to connect with new devices to ensure IPv6 requirements are met before deploying to VA network.

3.5 Operations and Maintenance

While the planning, equipment refresh, training and testing are in progress we will need to plan for the ultimate hand-off of network operations and maintenance of the IPv6 deployment. We will need to address maintaining a scalable configuration and change management. To do that, several supporting activities will be involved.

- Tools and processes for Network and Application Monitoring
- IP Address Allocation and Management
- Policy and Procedure Development
- Service Level Agreements to support maintenance activities and issue resolution
- Coordinated handoffs of Roles and Responsibilities

3.5.1 Tools and Processes

While tools exist today to support detection of equipment/network issues or application outages they will need to be examined for how they will make the transition to support IPv6. If those tools need to be replaced or upgraded there will be training needed in addition to acquiring new tools.

3.5.2 IP Address Allocation and Management

VA currently handles management of its existing IP address using a variety of methods in each region. This will not be a feasible approach with IPv6 due its vast increase in size of address space. VA will need to transition from the manual tracking and allocation of IP addresses to a more scalable method by evaluating, selecting and purchasing an IP Address Management (IPAM) tool.

3.5.3 Policy and Procedure Development

As the deployment of IPv6 matures, there will need to be changes or additions to policies on security, change management, maintenance support response frequency and procedural steps based on VA's preferred management approach.

3.5.4 Service Level Agreements

Existing Service Level Agreements (SLA) and contractual support agreements will need to be examined and if necessary, negotiated by VA for changes needed.

3.5.5 Coordinated Handoffs

Roles of the Transition Office and that of the working group members will need to be coordinated. Also those roles of staff to run the network will need to be coordinated. This role and responsibility handoff will also be dependent on appropriate training taking place.

4 RISK ANALYSIS

In performing the Risk Analysis, the risks arising from the deployment of IPv6 were identified, assessed, and quantified. The identified risks were then rated from Non-Critical to Most-Critical (see ***Appendix A – Summary of Risk Criticality***). The Risk Analysis is reported for risks classified into the following categories:

- ✓ Schedule
- ✓ Technical obsolescence
- ✓ Feasibility
- ✓ Reliability of systems
- ✓ Dependencies and interoperability issues
- ✓ Surety (asset protection) considerations
- ✓ Risk of creating a monopoly for future procurements
- ✓ Capability of agency to manage the investment
- ✓ Overall risk of investment failure
- ✓ Organizational and change management
- ✓ Business
- ✓ Data/info
- ✓ Technology
- ✓ Strategic
- ✓ Security
- ✓ Privacy
- ✓ Project resources
- ✓ Human capital

A summary of the risks and mitigation strategies can be found in ***Appendix C – Summary of Risks***.

These sections will be updated on a quarterly basis based starting April 2009- beyond.

4.1 Risk 1 – Schedule

Date Identified	Description of Risk ***Ipv6-Specific Consideration***	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk that the project will not meet all or parts of its list of terminal elements with assigned start and finish dates, such as release(s), milestone(s), deliverable(s), or critical task(s). ***This will reflect on the transition to IPv6 as a whole.***	Low	Sufficient funding and appropriate staff resources will be made available to the IPv6 transition effort. **Update** Funding proposal for FY 09-14 has been submitted. Transition scheduled to occur over five year period so as to minimize impact to any one group.	Government and contractor resources are being applied for the planning, transition, and testing of IPv6 capability. Responses to a data call for an inventory of IP-aware devices have been processed with ongoing updates.	Med

4.1.1 Key Considerations

Schedule impact is a composite of several other impact areas, as diverse considerations can translate into an impact on schedule. For example, all IP-aware devices in VA backbone must be IPv6-capable, either when initially acquired or when field upgraded. Since this transition to IPv6-capable devices will require time and resources, the schedule can be affected.

Another area that can affect the schedule is that of reliability. For example, if devices running in a dual stack IPv4/IPv6 environment develop reliability problems, these devices must be corrected or replaced. Or, perhaps, they will have to be configured differently. We expect this

to occur in isolated instances and not be a systemic risk. Correcting these anomalies will require time and resources.

Training can also impact the schedule. If training programs are not completed in time or if staffing and resources are unavailable to conduct training, the schedule could be impacted, causing lack of adequate stakeholder and user community involvement.[1]

There is a risk that thoroughly evaluating all purchases of IP-aware devices for IPv6 compliance may slow the purchasing process. Currently, the procurement process includes a requirement for IP-aware devices to be IPv6-capable. The vendor can respond either that the product to be delivered is IPv6-capable or that the product will be made IPv6-capable within a period of time. If VA were to place more precise requirements on vendors for IPv6 capability, or if testing is required in the acquisition process, the schedule can be affected.[2]

Staff responsible for implementing IPv6 could be overwhelmed with assignments considered more critical (such as network security and high-impact operational responsibilities) than the IPv6 transition.

VA is a decentralized organization which has autonomous regions. There may be a risk that if the regions do not comply with the OMB mandate in time, the schedule may be impacted.[3]

4.1.2 Mitigation

Mitigation of schedule impact will be accomplished in each of the impact areas that can affect schedule. These include the following:

- Provide adequate training of executives, managers, and staff personnel on IPv6 deployment topics. Training programs have been developed and an initial roll-out of Executive, Technical and Architecture focus has been addressed. This will need to continue.
- Identify and develop expertise with specific individuals who can function locally as reliable IPv6 knowledge experts assisting with train-the-trainer sessions, helping with the transition effort, answering questions, and demystifying the transition process. Train-the-trainer sessions have started and will continue as regions are identified.
- Get the maximum impact from training materials (classes, presentations, guides, white papers, etc.) by incorporating them onto a web site or portal targeted at the IPv6 transition community within VA. VA intranet has been updated periodically with transition progress and training materials.

To mitigate the schedule impact from verifying the IPv6 capability of newly acquired or upgraded products, we will review evaluation results obtained by other government organizations where applicable to VA requirements. We have established inter-agency meetings and will be starting a Technology Advisory Panel to share agency experiences and evaluations.

[1] Susan Hotzler, Program Manager, Employee Education System, Minneapolis Center
[2] Sandi Hughes, Management Analyst, VA Office of Information and Technology; James Carlson, Telecommunications Specialist, VA Office of Information and Technology
[3] Andrew DeLong, Network Engineer, VA Office of Information & Telecommunications/ IT Operations

Ensure through upper management that the regions comply with mandate.

Estimate time and resources required to ensure IPv6 compliance and create a realistic schedule for accomplishing this.

Establish and track frequent milestones to ensure the entire enterprise is making appropriate progress. Regions that fall behind schedule will be identified and their compliance will be expedited.

4.2 Risk 2 - Technical Obsolescence

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk that key technologies used in a project will lose value because a new, more functional product or technology has superseded the project's (e.g., cell phones versus the Blackberry) or when the project's product(s) become less useful or useless due to changes in other products (e.g., BETA or VHS tapes when everyone has CD or DVD players) before the project has completed its full functional life-cycle. *Hardware and systems that do not support IPv6 are not replaced before they are technically obsolete.* *Purchases occur of IP-aware devices for the backbone network that are not IPv6-compliant.*	Medium	Most routers and switches that will not support IPv6 will be replaced as part of normal technology refresh processes. These were identified in VA IPv6 inventory. Some security and network management devices may need to be replaced to meet IPv6-capability requirements.	It is expected almost all routers and switches will support IPv6 although many security and network management systems may not be ready in time. It is possible that until all vendors have upgraded their hardware, IP-aware devices that are not IPv6 compliant may be purchased. However, it is not expected purchases will be made that impact fulfilling the OMB mandate requirements, since these devices would not be employed in VA backbone.	High

4.2.1 Key Considerations

One of the most important activities at this stage of the IPv6 transition is ensuring that purchases of IP-based equipment and software are IPv6-compliant. The mere act of multiple large federal government agencies asking the "IPv6-compliant" question will motivate vendors of IP-aware products to put serious consideration into ensuring their products are IPv6-capable. The success of the IPv6 transition will be heavily dependent on the efforts of manufacturers to make their products IPv6-compliant.

The right criteria must be used in evaluating purchasing options. It is one thing for a vendor to mark a checkbox that their equipment is IPv6-compliant and it is something completely different to have confidence that the equipment will meet VA requirements for IPv6 compliance. Something equivalent to an entity certifying that a product is IPv6-compliant (such as the "IPv6-

Ready" effort) could greatly reduce potential problems when IPv6 is enabled. Although VA is not aware of single definitive "stamp of approval" at this time, the government has some certification requirements and policies under FIPS, FISMA, and NIST IPv6 Profile.

It is reasonable to assume that IP-aware equipment that represents considerable long-term investment will require in-house IPv6 compliance testing in addition to a "certification" from a certification or testing entity. For example, evaluation of an enterprise Voice over IP (VoIP) solution must include evaluation of IPv6 capabilities and compliance to ensure that the solution will meet VA functionality and performance requirements. It is also likely that a certification organization will focus initially on mainstream IP-enabled products and that "niche" products such as IP-enabled medical equipment must be evaluated by VA.[4]

Purchasing rules regarding IPv6-compliance must be flexible enough to empower purchasing the best products to support the core missions of VA. Consider the situation where a specific class of IP-aware biomedical device is being purchased and both IPv6-compliant and non-IPv6-compliant devices are available. It may be in the best interests of VA's customers to select a non-IPv6-compliant device if it was otherwise the superior and most cost-effective product in its class. Waiving the IPv6 requirement should only be done after carefully evaluating the pros and cons of each option, including the impact of the proposed wavier on long-term transition strategy.

The majority of the IP-aware devices most recently purchased in VA have been under a contract vehicle identified as SEWP IV (NASA-National Aeronautics and Space Administration/ Solutions for Enterprise-Wide Procurement – Current designation: December 18, 2006 for five years until December 17, 2011) or under GSA federal schedule contract. Prior to that, the majority of IP-aware devices purchased in VA were obtained under a contract called PCHS-2 (VA Procurement of Computer Hardware and Software -2) vehicle, although some IT equipment was also obtained under GSA. Under Each contract note: SEWPIV, GSA and PCHS-2;; all vendors have been notified that after January 1, 2006, all equipment that is added to the contract be IPv6-compliant or that the supplier have a roadmap for the product to become IPv6-compliant.

Risks that exist in VA purchasing process include:

- Vendors are not required to meet any specific criteria in their statements that IP-aware devices are IPv6-compliant or that there is a roadmap for becoming IPv6-compliant.
- For IP-aware devices added to any contract before January 1, 2006, vendors are not required to document IPv6-compliantce nor to provide a roadmap to become IPv6-compliant.
- Specialized IP-aware devices (such as routers or security equipment with unique component lists) are not part of any contract and the process for evaluating these products for IPv6-compliance is unclear. This said, those who recommend and authorize purchases of backbone network IP-aware devices are aware of the requirement for IPv6-compliant devices on the backbone network.

[4] VA already has a laboratory for evaluating the security characteristics of medical devices. The activities of this lab could be expanded to address IPv6 evaluation.

- Purchases of IP-aware devices that fall outside the realm of conventional IT products (such as IP-aware biomedical equipment) may occur via the purchasing organizations within VA regions. It is not clear if verification of IPv6-compliance (or a roadmap for IPv6-compliance) is requested.
- Equipment classified as telecommunications equipment is not part of any contract at this time. However, telecommunications vendors are required to document IPv6-compliance or to provide a roadmap to become IPv6-compliant.[5]

4.2.2 Mitigation

A comprehensive purchasing policy must be developed for ensuring IPv6-compliant devices are purchased across VA organization. Purchasing organizations across VA organization, particularly those in regions, must be trained to identify IP-aware devices and to verify IPv6-compliance.

Random audits of IP-aware device purchases must be conducted at all purchasing levels of VA to ensure that the devices purchased were evaluated for IPv6-compliance.

IP-aware devices on VA backbone network that are not IPv6-compliant and will have a direct impact on VA's ability to fulfill the requirements of the OMB mandate will be replaced.

There must be a concerted effort to encourage all vendors and manufacturers of all IP-aware devices to make serious efforts to make their products IPv6-compliant. This may require a unique outreach to vendors and manufacturers for which it is not clear how VA can or should contribute.

4.3 Risk 3 - Feasibility

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk that a process, design, procedure, or plan cannot be successfully accomplished in the required time frame as proposed. *The planned IPv6 capability does not function as expected.*	Low	Evaluate existing implementations that are similar to that being attempted by VA. Establish relations with groups, organizations, associations, vendors, and other agencies that are deploying or have successfully implemented IPv6. Ensure that technical and managerial personnel have the capability to successfully develop and implement the project. Ensure that all personnel involved with the project are properly trained in a timely manner.	IPv6 PMTO is working with several agencies to do knowledge sharing. Subgroups have been formed for IPv6 transition. VA and contracted staff have attended IPv6 conferences and are making contacts with other IPv6 implementers. Cost estimates for training have been developed.	Medium

[5] Sandi Hughes; James Carlson

4.3.1 Key Considerations

The required functionality of network devices, management tools, and security tools would be insufficient to simply activate the IPv6 capability on VA backbone. In addition to the availability of IPv6-compliant products, training of personnel to install, manage, and evaluate the network after it has been made IPv6-capable will be a necessary component. Prior to activation of IPv6 on VA backbone, the change of network components must be documented, evaluated for security, and certified for use. Examples of feasibility risks include:

- Management and/or security tools that are not IPv6 capable, are not at the required release level, or are insufficiently mature to warrant deployment.
- Equipment and tools are available, but the technical staff lack adequate training.

4.3.2 Mitigation

VA working groups will seek out other implementations, regardless of maturity level, that are similar or mirror VA's planned IPv6 transition approach. It will be important to learn what works and what does not work in these implementations.

In general, VA will establish relations with groups, organizations, associations, vendors, and other agencies that are deploying or have successfully implemented IPv6. The IPv6 Transition office has conducted an initial Inter-agency meeting with GSA, DoD/MHS, DOE, DOL, DOJ for discussion of successes and common issues. Continued attendance by VA representatives at federally targeted IPv6 meetings and workshops will form a part of the knowledge acquisition process that will assist in planning VA's IPv6 transition.

It is critical to ensure that technical and managerial personnel have the capability to successfully develop and implement the project and that all personnel with the project are properly trained in a timely manner.

An end-user (clinician, etc) feedback mechanism must be in place to resolve issues. Initially, user feedback will be gathered and recorded during training and awareness activities.

Sufficient lead time must be built in the implementation schedule to allow for training and security certification network staff.

4.4 Risk 4 – Reliability of Systems

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Impact
May 2006	The risk that the system, when operating under stated conditions will not perform its intended function acceptably for a specified period of time. *Risk that hardware and systems operating in a dual stack IPv4/IPv6 (the likely VA IPv6 goal deployment architecture) environment are less*	Medium	Extensive testing in a lab environment to verify reliability of dual stack systems. Where reliability is not commensurate with that of IPv4-only systems, these issues will be investigated and where appropriate, discussed and resolved with hardware and systems vendors.	Basic testing has been completed. VA is reviewing NIST IPv6 Test Program. Also, we are following the JITC certifications as they become available.	High

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Impact
	reliable than IPv4-only systems.				

4.4.1 Key Considerations

Risks associated with IPv6 have shifted to post-June 2008.[6] Pre-June 2008 risks are concerned with being able to provide basic, secure IPv6 capability on VA's backbone network. Post-June 2008 risks go beyond basic IPv6 capability and include focus on IPv6-enabling VA production systems and applications and exploring potential IPv6 benefits in greater detail. (Related topic: *Risk 11 - Business*).

It is important as changes are made to the network that no disruption or degradation of service occurs, especially for an application with life-critical functionality. This risk could be realized directly when a malfunctioning IPv6 device is introduced into the network, or indirectly when technical staff is diverted from ongoing network maintenance to perform IPv6-related tasks.

For example, DNS considerations in a campus environment can lead to a variety of problems. Users experiencing network delays attempting to reach a host with excellent IPv4 connectivity may perceive that enabling IPv6 on their computers has 'broken' the overall network environment. This user perception can lead to an enterprise-wide impact, such as excessive call center activity or network overload due to address seeking. Further examples of this situation include:

- Undesirable client DNS interactions may occur in a dual stack deployment environment where there are pockets of IPv4-only and dual stack networks (Reference RFC 4472)
- Incorrect responses from DNS servers regarding IPv6 address queries may confuse DNS clients (Reference RFC 4472).

It is believed that the IPv6 protocol features and capabilities are not yet mature, mainly because standards are still under development and have not been tested in widespread production implementations. Consequently, although IPv6 installations exist, there is still a lack of sufficient IPv6 installations running in a production mode to benchmark for reliable production data. These statements will be particularly relevant when IPv6 deployment is attempted more aggressively in LAN environments with applications and users. Historically, there are many examples of cases where network administrator reliability concerns have impacted the widespread deployment of IPv6 beyond the backbone network.[7]

4.4.2 Mitigation

Each implementation has its own needs and requirements. VA IPv6 workgroups are continually developing test plans, measures and methods and will leverage pre-existing test data and results where available. The transition team will also develop a specific set of tests to establish

[6] VA was ready for IPv6 on the backbone several months before June 2008.
[7] IPv6 Deployment Guide: http://www.6net.org/book/deployment-guide.pdf; page 333, William Cerveny, "Internet2 and IPv6" presentation at December 2005 IPv6 Summit, http://www.wjcerveny.com/2005-12-IPv6-Summit-v1-1.pdf, slides 28 and 29

reliability standards. Reliability of systems risks will be mitigated primarily by using concise definitions of requirements and testing. A solid definition of requirements is mandatory for building an appropriate test plan and in execution of the tests.

In planning changes to the network, it will be important to test new components sufficiently under laboratory conditions prior to placing them into the backbone. Since disruption of critical functionality must be absolutely avoided, steps must be taken to isolate new components from production traffic until it can be assured that reliability, security, and performance requirements are being met.

Both positive testing (that the item functions to specifications when exercised in the expected ways) and negative testing (that the item fails in acceptable manners when exercised in unexpected ways) will be necessary.

Where reliability is not commensurate with expected requirements, investigating and discussing these shortcomings with hardware and systems vendors should be done to establish a resolution.

Related mitigation topics can be found in the discussion for business risks (*Risk 11 - Business*).

4.5 Risk 5 - Dependencies and Interoperability Issues

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The project will fail because it depends upon the successful completion of another system or the project will not be able to work with other systems or products without an unplanned special effort. *Other organizations and vendors critical to IPv6 readiness will not support IPv6 Transition activities.* *The risk that the goals of the project do not coincide with the goals of other projects.*	Medium	ISPs and other organizations' networks that VA backbone network peers with will be encouraged to deploy IPv6. For the June 2008 time frame, VA backbone was not dependent on being able to interoperate with other external networks. Careful planning and cooperation must occur between other projects that have components that are IP-aware.	VA is in the process of transitioning to Networx telecommunications provider services that are better able to address IPv6 interoperability. We have been in contact with several ISPs to determine their readiness. While they are not yet ready to offer public IPv6 support we continue to monitor their progress. The IPv6 PMTO will be developing a deployment plan to integrate other major initiatives into the overall project schedule	High

4.5.1 Key Considerations

For the June 2008 mandate, VA needed to verify that their network will have interoperability with the external IPv6 enabled internet. VA met the June 2008 mandate. In addition, it conducted additional testing with other agencies. When VA's IPv6 transition progresses beyond the boundaries of the backbone network, there will need to be testing to ensure that backbone routers can interoperate with the routers of peer and transit networks, such as for commodity

Internet services and for connections to universities or other government agencies. (Peer connections that exist between VA LANs and the LANs of other organizations occur at the campus level and are not considered part of VA backbone network).

There is a risk that the goals of this project do not coincide with the goals of other projects, such as projects that may implement solutions that are only supported with IPv4.

4.5.2 Mitigation

Conducting both positive testing (that the item functions to specifications when exercised in the expected ways) and negative testing (that the item fails in acceptable manners when exercised in unexpected ways) will be important in testing dependencies and interoperability issues. Testing will need to occur in both a test lab environment and in a controlled environment on the production VA network.

Mitigation of network interoperability issues will require providing the peer/transit network's staff with identification of the issue to enable them to develop a solution. Likewise, mitigation of device/system dependency and interoperability issues will require providing the vendor or manufacturer with identification of the issue to enable them to develop a solution. If the vendor or manufacturer is unable to solve the issue, the product will need to be replaced by a compatible product.

It will be critical that this project be coordinated with other projects that rely upon the backbone network. For example, it must be ensured that any project that would introduce new security or privacy devices onto the backbone network would interoperate with IPv6 in a dual stack/native environment. VA IPv6 Transition Work Group is in a position to accomplish this coordination.

4.6 Risk 6 - Surety (Asset Protection) Considerations

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk of the project to meet its obligations or when public or private interests require protection from the consequences of a contractor's default or a project's delinquency. *Key VA and/or contractor contributors default on project milestones or project work products are destroyed.*	Medium	Ongoing and frequent meetings and publication of deliverables and deliverable updates. Ensure adequate disaster recovery procedures are in place.	Project conducts frequent status updates and is using existing protection mechanisms available to the project.	Medium

4.6.1 Key Considerations

A failure to exercise due diligence in carrying out IPv6 transition tasks could result in a loss to some public or private interest.

For example, errors made in delivering the required products to VA or contractors missing delivery requirements due to the lack of qualified staff. Other scenarios may be that VA management fails to make required decisions in a timely manner, that project management fails to track key product deliverables or that a supplier may misrepresent capabilities of products or technologies and that these situations are not promptly addressed.

Networks are vulnerable to a variety of unforeseen disasters that may impact not only the deployment of IPv6 but also the infrastructure itself. The disruption of operations may range from mild such as short-term equipment failure, power outage, to severe facility failure such as fire, earthquake, destruction of the infrastructure, etc. This risk is also part of the assessment for Information Assurance (IA).

4.6.2 Mitigation

To mitigate this risk, contractual requirements must include specific performance and delivery items that reflect quality and timeliness criteria. Project management techniques must be used to define schedules and deliverables and to monitor their timely and appropriate completion.

Frequent meetings and teleconferences along with collaboration tools will facilitate communication among responsible parties. Identifying potential problems early and tracking their resolution as action items with priorities and due dates are essential. Identifying alternative means of accomplishing key milestones and activating the alternatives in sufficient time to preserve overall schedule must be completed.

Effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. Agency management must ensure the development not only of a contingency plan, but also of a business impact analysis, of preventive controls, of training, testing, and exercises as well as a maintenance plan according to policies already established by the agency. A security plan also is being developed that documents the management, technical, and operational controls of information systems according to federal standards.

4.7 Risk 7 - Risk of Creating a Monopoly for Future Procurements

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk associated with the use of closed or proprietary software/source code, as well as the dependence on a single vendor or product which in turn creates a risk that in the future the contractor will be able to reap windfall profits by charging excessive costs or reducing service quality. *Using routers from a single vendor leads to a risk of higher costs or reduced service quality because of a lack of competition.*	Low	All routers on the backbone are from a internationally recognized single vendor. However, these routers conform to standards that enable them to successfully interoperate with networks outside VA. If desired, these routers could be replaced with routers provided by other vendors; however, this would promote difficulties dealing with multiple vendors, require differing staff skills, and increase complexity in the procurement process.	VA has accepted this risk because other considerations offset risk. These include avoiding difficulties dealing with multiple vendors, reducing the type of staff skills needed, and avoiding complexity in the procurement process.	Low

4.7.1 Key Considerations

A single company or group of companies with monopoly power in the market for IPv6 products could delay or impede the normal dissemination of IPv6 by charging excessive prices or reducing the service quality. Competitiveness is fundamental in the marketplace in order to avoid the dependency on a single vendor and the risk that in the future the contractor can manipulate profits.

Most stakeholders agree that the market is the primary driver for the adoption of IPv6 and that at this time there do not seem to be grounds to think that there is an IPv6 monopoly power. Moreover, new technologies seem to bring temporary monopolies as part of the normal deployment process. However, the risk exists and measures, safeguards, and controls must be taken to mitigate it.

VA backbone is exclusively a Cisco implementation. Continuation with this single-vendor implementation may affect the ability of the Department to procure different equipment in the future, to buy it at a fair market price, or to interoperate with other agencies or groups that use a different vendor.

4.7.2 Mitigation

The risk of creating a monopoly for future procurements will be mitigated by using products that adhere to standards for interoperability and management. VA will strive to comply with IETF best current practices for IPv6 as well as research vendors that comply with the NIST Profile for IPv6.[8] In addition, since complete interoperability will be a long process, VA must over time ensure interoperability with key agencies and groups to minimize problems. The decision to have one manufacturer in the backbone is mitigated by the overwhelming advantages of enhanced interoperability, simplified training, and added value offered by the manufacturer via proprietary solutions. The manufacturer used provides outstanding leadership in the IPv6 standards area.[9]

4.8 Risk 8 - Capability of Agency to Manage the Investment

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	Risk associated with an inexperienced project owner and management team, or the lack of established OMB approved management tools, or performance indicators that show that the Department cannot deliver the project as promised. *Inability of*	Low	Assignment of experienced managers with prior IPv6 implementation experience and proven monitoring and reporting tools to the IPv6 transition effort. Sufficient time will be added to schedule to allow for slippage in the schedule.	Experienced management is being applied to IPv6 transition.	Medium

[8] NIST Special Publication 500-267

[11] For example, Cisco representatives have authored or co-authored RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification, RFC 3633 - IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6, and RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
	management to manage priorities within resource constraints to reach the IPv6 deployment goal.				

4.8.1 Key Considerations

During the course of the IPv6 transition, VA management may encounter obstacles in managing resources and priorities. Examples of factors contributing to this risk include the following:

- Assumptions are made concerning anticipated availability of products or project resources that turn out not to be valid
- Sub-optimal management tools are used to measure project performance that fail to reveal serious incompatibilities or inadequacies in meeting requirements
- Sub-optimal communication among VA organizational units results in failure to agree on addressing conventions or resource allocations
- Sub-optimal assignment of priorities to project activities results in critical results not being available on time

This risk is closely related to *Risk 1 – Schedule* and *Risk 6 - Surety*.

4.8.2 Mitigation

VA has embarked upon the IPv6 transition effort with a multi-faceted approach designed to mitigate risks in this area. By opening up communication channels early in the project and by leveraging the specific knowledge of talented VA employees, VA is taking the first steps to mitigate the risks in this area.

- Assignment of experienced managers with proven monitoring and reporting tools to the IPv6 transition effort.
- Provide sufficient time in schedule to allow for controlled slippage where justified.
- Include specific performance and delivery items in contracts that reflect quality and timeliness criteria.
- Use project management techniques based on the Project Management Institute's Project Management Body of Knowledge (PMBOK) and other industry best practices to define schedules and deliverables and to monitor their timely and appropriate completion.
- Use frequent meetings and teleconferences along with collaboration tools to facilitate communication among responsible parties.
- Identify potential problems early and track their resolution as action items with priorities and due dates.
- Identify alternative means of accomplishing key milestones and activate the alternatives in sufficient time to preserve overall schedule.

4.9 Risk 9 - Overall Risk of Investment Failure

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	This risk refers to the potential that there is an inherent project weakness such as the project missing a clear link between it and the organization's key strategic priorities, including agreed measures of success. *Lack of alignment of IPv6 transition components with VA strategic IT goals, objectives, and performance measures.*	Low	Alignment of IPv6 transition with VA strategic IT goals, objectives, and performance measures. Tracking IPv6 implementation projects using relevant performance measures to control schedule, cost, and quality.	IPv6 transition is recognized and incorporated into VA Enterprise Architecture.	Medium

4.9.1 Key Considerations

Incorrect assumptions as to the IPv6 project strategy could result in a failure to meet the IPv6 transition objectives. This risk could present itself, for example, if the project owners spend too much time on the smaller, tactical issues rather than the larger, longer-range strategic ones. It may also be that the project owners pursue objectives outside the scope of the agency's Strategic Plan. Alternatively, customers of the project's deliverables may not be satisfied with the desired solution.

4.9.2 Mitigation

It is human nature to default to those tactics with which we feel most comfortable. Goals should not be confused with plans. Moreover, a set of goals is not a strategy. Therefore, the stakeholders must ensure that the IPv6 transition has not only a clear set of goals but also a strategy capable of meeting the agency's goals and objectives.

Training of key personnel and communication to VA community on transition goals and progress is extremely important to successfully manage the effort. Along the same lines it is also important to provide adequate resources to manage the transition and future maintenance.

Reviewing IPv6 strategies and assumptions at key points in the implementation to make appropriate course corrections in a timely manner will diminish the risk of failure.

4.10 Risk 10 - Organizational and Change Management

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	Risk that activities involved in (1) defining and instilling new values, attitudes, norms, and behaviors within an organization that support new ways of doing work and	Low	Adjustments to the project will be made to compensate for any organizational changes.	VA has changed CIO, but the functional direction of the organization is in place. Potential IP Address Management tools are	Low

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
	overcome resistance to change; (2) building consensus among customers and stakeholders on specific changes designed to better meet their needs; and (3) planning, testing, and implementing all aspects of the transition from one organizational structure or business process to another, will not be successful.			being evaluated with potential re-organization scenarios as an evaluation criteria	
	IPv6 transition and its operation cause organizational and individual disruptions or dislocations. VA organizational changes may cause variations in the scale and nature of the project (training budget is one example).				

4.10.1 Key Considerations

IPv6 running on the infrastructure is not expected to require line organizations and individuals to change how they function. Since the level at which IPv6 operates is below the day-to-day concern of the end user, organizational and change management considerations are expected to arise only within the organizations that deal directly with the communications infrastructure. This pertains to the transition from IPv4 to IPv4/IPv6 and ultimately to nativeIPv6 operation. A focus of the transition plan has been to ensure End-Users will not experience any detrimental impact in using IPv6.

Following achievement of IPv6 capability on VA communications backbone, user organizations will have visibility into the IPv6 transition as it will then be possible to capitalize on the benefits of IPv6. Planning will be required of these organizations to make decisions and identify strategies for use of capabilities such as end-to-end addressing and IP Security.

4.10.2 Mitigation

When IPv6 enhanced functionality is available post-2008, VA and contractor personnel will be educated regarding the implications of IPv6 in VA. Potential impacts on VA personnel and organizations will be identified well before it is necessary to accomplish significant changes in attitudes, behaviors, and activities. Tools used to manage network IP addressing are using re-organization scenarios as evaluation criteria to determine how well the tool can help network managers adapt to organizational and network management situations. All plans and initiatives have been proposed to be completely seamless and transparent to any End-User, with any component, device or service using IPv6.

4.11 Risk 11 - Business

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	Business risk is the potential that an investment will fail to achieve the expectations of the project's owners and customers. *IPv6 benefits such as better security and reduced management costs are not realized.*	Low	Research and testing will be conducted to verify or refute claimed business benefits and explore new business benefits. Steady communication of progress and tangible benefits to VA user community.	Planning to mitigate business risk has been initiated. Newsletters and VA Intranet sites have been distributed or created to notify VA community of the progress and benefits of IPv6	Medium

4.11.1 Key Considerations

The risk that the investment fails to deliver the user's expectations is a business risk associated with any new technological implementation. All technologies follow a learning curve. When IPv4 was first introduced it was not the protocol we know today; many of the features were introduced as the protocol evolved.

Today we want to replace a protocol that was never created to deliver the functionality of today's demanding applications. IPv6 was developed out of the experiences acquired with IPv4 but is still in evolution. Therefore some of the features and functionalities will come in later years.

Although the general rationale for the deployment of IPv6 has been the exhaustion of the IPv4 address space, not everybody seems to share this view. Even in Japan, one of the first IPv6 adopters, there seems to be dissent.[10] In the United States there is also a difference of opinion.[11] However, globally, address space exhaustion is probably the single most important reason for the development and adoption of IPv6. Experts in the field vary in their predictions, but one prediction is that the IPv4 address space will be exhausted by 2012.

The size of an address in IPv6 is 128 bits, i.e., four times longer than the 32-bit IPv4 address. A 32-bit address allows for 4,294,967,296 possible addresses. A 128-bit address allows for 340,282,366,920,938,463,374,607,431,768,211,456 possible addresses (approximately 3.4×10^{35}).[12] The benefit of the immense number of IP addresses is the availability of addresses to support the emergence of new services and applications that require large quantities of globally routable internet addresses.

In addition to address space exhaustion, IPv6 provides many other benefits to the business as outlined below:

- **Increased Security and Spam prevention due to end-to-end addressing** - The IPsec (Internet Protocol Security) protocol will provide several security functions such as Access Control List (ACL) access to individuals who have authorization.

12 Is IPv6 necessary? - Nobuo Ikeda, Hajime Yamada

13 A pragmatic Report on IPv4 Address Space Consumption – Tony Hain

14 For comparison purposes, NASA Godard Space Flight Center provides an estimate that there are 10^{21} stars in the universe (1,000,000,000,000,000,000,000). And the Journal of Modern problem solving provides an estimate that there are 7.5×10^{18} grains of sand on all the beaches of the earth (7,500,000,000,000,000,000).

- **Multiple Hierarchy Levels** - This will help aggregate routes, facilitating efficiency and scalability. The practical benefit is that organizations may have a tiered network hierarchy improving address space management.

- **Improved Quality of Service (QoS)** – Although considerably more work must be done in the development of QoS standards, this feature will potentially allow users to prioritize traffic. IPv4 is a best effort scheme i.e. data, voice, and video are treated with the same priority. IPv6 contains a field, the *flow label* that is not found in IPv4 which allows routers along the connection to treat traffic with greater specificity or granularity. This can be very useful, for example, for streaming applications such as video conferencing and VoIP that require real-time data transmission.

- **Autoconfiguration** - This feature will allow nodes of the IPv6 network to configure their IPv6 addresses. This is an IPv6 feature that allows an IPv6 host to append its link-layer address, an Ethernet MAC address for example, to a unique unicast IPv6 prefix advertised on the local link. This feature enables plug and play which identifies and connects devices to a network without the need of a DHCP server.

- **Simplify Mobility** - This capability will help satisfy the increased demand of emerging mobile or portable applications. This is an important feature for users who need access to the World Wide Web, home, e-mail, etc. from outside these networks using Layer 2 wireless technologies such as 3G. The Mobile IP protocol solves this problem by allowing nodes to move freely from one IP network to another without losing data or interrupting computer applications and settings. Mobile IPv6 is built into the protocol, for IPv4 is an added function.

- **Increased Network Efficiency** - IP was originally designed to be an end-to end protocol i.e. only hosts are capable of handling the connection. The use of network address translation (NAT) breaks this model. It also inhibits end-to-end network security and hinders network performance since it requires additional processing to do address translation. After transitioning to IPv6, NATs can be removed and there will be fewer processing steps and transmission bottlenecks.[13]

All these improvements will not be immediate, but will be implemented as the protocol matures, so the return on investment is a long-term plan.

In summary, although there may be a risk that the investment may fail, the implementation of IPv6 is inevitable because IPv4 will not be able to deliver the services that the market is asking for. The question is not whether one should consider IPv6, but when is the right time to implement it and what is the best way to do it.

[13] See IETF Internet-Draft "IPv6 Network Architecture Protection," http://www.ietf.org/internet-drafts/draft-ietf-v6ops-nap-02.txt for a discussion of how IPv6 can be used to provide the same security and management benefits associated with NATs.

4.11.2 Mitigation

As mentioned before, IPv6 is a protocol still in evolution and consequently the measure of its success will depend upon the needs and requirements of the specific network being implemented. In order to minimize impacts to VA's mission, the following measures should be taken:

- **Define current standards for "IPv6-compliant" devices and functional specifications.** Different vendors have different definitions of what IPv6-compliant means. Each organization must develop standards for IPv6-compliant devices and functional specifications that conform to its needs and requirements. By doing so, the agency will set the correct expectations for a successful implementation. (See *Risk 4 – Reliability of Systems*). To help drive toward an equipment standard we will use the NIST Profile (NIST Special Publication 500-267). This reference defines IPv6 "basic capabilities" for infrastructure devices.

- **Define future standards for "IPv6-compliant" devices and functional specifications as IPv6 evolves.** The transition to IPv6 will be a long-term evolution. Some of the benefits that IPv6 brings will materialize in the future when the protocol becomes fully interoperable and implemented end-to-end. As the evolution of the IPv6 implementation continues, the organization must set milestones that define what the future features and functional specifications will be.

- **Align VA's various business goals with the potential benefits of adopting IPv6.** Once the business needs have been identified, they must be prioritized in a plan for IPv6 implementation after IPv6 is enabled on VA backbone. For example, the VHA Home Telehealth program may benefit from the ability to establish an IPv6 network that encompasses the veteran's home monitoring equipment and VA servers.

- **Implement a test platform to verify reliability of transition mechanisms.** A test bed is very important to extend research into realistic network environments, to build a system with common components, to create a teaching platform, and to build research collaborations. In VA's case, it will, above all, help tremendously to verify the reliability of the IPv6 transition mechanisms. Pilot tests are being developed to apply IPv6 related benefits to existing Telehealth patient an hospital programs applications. The planned pilots will demonstrate a viable and obvious gain by using IPv6.

- **Conduct research and testing to verify or refute claimed business benefits.** In order to minimize risk, new IPv6-based functions or applications must be fully researched and tested prior to implementation to avoid any negative impact on the network. Vendors' claims must be fully tested to confirm or reject the veracity of the benefits.

4.12 Risk 12 - Data/Info

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	Risk associated with data/information loss or disruptions caused by natural disasters (hurricanes, tornadoes, floods,	Low	Early lab test and production backbone network test should identify un-inventoried IP-aware devices. These assets will	IP-aware devices in VA backbone that must support IPv6 have been inventoried and it is believed that their IPv6-	Medium

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
	earthquakes, etc.) or by area-wide disruptions of communication or electric power or malicious attacks. In addition, it can also include the ability of the investment to obtain, store, produce, share, and manipulate data as planned.		be upgraded and made IPv6-compliant or, be replaced or removed.	compliance status has been correctly identified. In addition, VA continues to progress through planned asset refreshment and inventory assessment.	
	IP-aware hardware and systems that must be IPv6-capable to support the mandate are not identified in inventories. *The process of making IP-aware devices IPv6-capable causes disruptions.*				

4.12.1 Key Considerations

IPv6-compliant products are not expected to introduce data or information vulnerabilities that are greater than those existent with IPv4-only products.

It is possible that the process of upgrading the software on an IP-aware device (such as a router) to support IPv6 and enabling IPv6 on the device may introduce unexpected behavior changes in the device. For example, enabling IPv6 capability and transiting IPv4 and IPv6 traffic across a router may markedly increase router memory consumption and the central processing unit (CPU) utilization. In addition to adversely impacting IPv6 network performance, IPv4 network performance could also be impacted to the extent that packets are dropped. This will certainly be a consideration on older Cisco 2500-, 2600-, and 3600-class routers if they are not replaced.[14]

It is not unheard of for software upgrades on routers to have bugs that are not detected in the manufacturer's extensive testing, particularly when the bug is related to enabling an advanced router or network feature. Some software bugs could cause IPv6 and IPv4 routing performance and functionality problems.

4.12.2 Mitigation

Early lab testing and controlled production backbone network testing should identify IP-aware devices that were missed in inventories. As with equipment already in the inventory, these newly identified devices will be made IPv6-compliant, replaced or removed.

To the extent feasible, specific software upgrades will be tested in a lab environment before they are attempted on production devices. Testing will include ensuring that the device's IPv4-handling behavior has not changed, evaluating router performance with the presence of IPv6

[14] Sean MacKirdy, National Account Manager,Department of Veterans Affairs, Cisco Systems, Inc.

traffic, and ensuring that enabling existing IPv4 capabilities with new IPv6 capabilities does not unleash software bugs.

The number of changes at one time should be minimized. For example, the router should be allowed to run without configuration changes (where possible) for a period of time before IPv6 capabilities are enabled on the router. This will expedite both recovery from a failure and identification of the specific change that caused the failure.

Vigilant tracking of Cisco advisories regarding release deprecations will be critical during the period when the IOS release on VA's Cisco routers are upgraded. Vigilant reporting of problems that can be attributed to hardware and software errors is also critical.

Vendor disaster recovery and fallback/rollback plans should be available in the event security, capacity, latency or other unforeseen issues adversely impact the backbone network.[15]

4.13 Risk 13 - Technology

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	This risk refers to the problems associated with the use of technologies new to the Department, new software releases, or hardware new to the market. *Risk that other advanced technologies, such as data encryption and QoS, are not fully supported in conjunction with IPv6.* *Potential for unavailability of mature IPv6 technology (lack of standards). Legacy applications that cannot be upgraded or made compliant with IPv6. Inadequate supply of IPv6 ready equipment or software creates monopolistic pricing environment.* *Risk that VA does not adequately define requirements for an IPv6-capable*	Medium	Identification of requirements, development of a test plan and lab testing of IPv6 used in conjunction with other advanced services will be completed. Training of Architectural and Network Management staff will continue in order to mitigate this risk.	Gaps in advanced services with IPv6 have not been evaluated extensively, although VA's preferred router/switch manufacturer is addressing gaps in their systems.	Medium

[15] Carl Foster, Telecom Specialist, VA Office of Information & Technology

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
	infrastructure.				

4.13.1 Key Considerations

To mitigate this risk, VA needs to establish a minimum set of standards, requirements, and procedures for testing.

Many routers and switches in VA backbone will support IPv6 after software upgrades. Some of these software upgrades will introduce changes in the way the router behaves and in the way the router's administrative interface appears. To correctly configure and maintain the upgraded routers, network administrators will need to understand the differences introduced by the software updates. Without appropriate reconfiguration, it is possible an upgraded router may fail to fulfill its IPv4 network requirements.

IPv6 configuration of routers will in general be straightforward for experienced network administrators. However, there may be situations which will confuse the network administrator. As a general example, in enabling IPv6 auto-configuration on a router and discovering the feature does not work, the network administrator may suspect a router malfunction; in actuality, the router is rejecting being configured in a manner inconsistent with IETF standards (as intended by the operating system developer). More time than expected may be spent on configuring a router's IPv6 capabilities.

It is possible a network administrator will configure IPv6 security policies similar to IPv4 security policies, without regard to IPv6 peculiarities. This will be sufficient in most cases, but in some cases IPv6-specific security vulnerabilities may be introduced.

If implemented, tunnel-based transition methods may create a combination of sub-optimal routing and security risks. For this reason, if they do become necessary, any tunnels should be strictly managed to preclude bypassing of security parameters.

At this time, many network management systems that support IPv6 do not support as many features of IPv6 as are available with IPv4. Some monitoring and measurement capabilities used with the IPv4 backbone network environment may not be available in the parallel IPv6 backbone network environment.

See also *Risk 12 – Data/Info*.

4.13.2 Mitigation

To mitigate technology risks, identification of a minimum acceptable set of IPv6 standards/requirements for the backbone network is underway and testing will be conducted to ensure the backbone network will support this minimum. NIST has also published an IPv6 Profile to assist Federal agencies with standards for acquisition of IPv6 technology.[16]

[16] NIST Special Publication 500-267

It will be essential to evaluate router operating system upgrades for "holistic" changes in how the upgrade changes the behavior of the router. These changes must be documented carefully and network administrators informed of potential problems before they attempt a router upgrade.

A combination of thorough training and post-training support will be essential in ensuring the network administrator has the knowledge necessary to successfully upgrade and configure routers to support IPv6. In addition to formal hands-on training opportunities, there will need to be forums (or equivalent mechanisms) for the administrator to both ask questions and find answers regarding IPv6-deployment issues in the field. Remedies for commonly encountered IPv6 problems must be fed back into the formal training process.

IPv6 traffic initially introduced onto the IPv6-enabled VA backbone network will not be critical or sensitive in nature. As familiarly and confidence with IPv6 grows and as IPv6 functionality solidifies across IP-aware devices, more traffic volume and more varied traffic types can and should be introduced.

Tunnel-based transition methods will be discouraged and avoided.

4.14 Risk 14 - Strategic

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk of misalignment with Department Mission and Strategic Goals, and/or the Presidents Management Agenda. *Risk that IPv6 backbone and WAN transition is not aligned with VA's strategic planning.*	Low	Alignment of IPv6 transition with VA strategic IT goals, objectives, and performance measures	IPv6 transition is recognized and incorporated into VA Enterprise Architecture.	Medium

4.14.1 Key Considerations

The potential exists that there will be a misalignment between IPv6 project components and VA strategic planning resulting in inadequate resources being applied to the project or a lack of appropriate management leadership.

There is a risk that the pervasive nature of IPv6 in VA infrastructure is not sufficiently recognized, resulting in a serious misalignment with competing demands on VA resources.

4.14.2 Mitigation

The IPv6 transition must be aligned with VA strategic IT goals, objectives, and performance measures. IPv6 capability falls within VA Strategic Plan Objective E-3: *Implement a One-VA information technology framework that supports the integration of information across business lines and that provides a source of consistent, reliable, accurate and secure information to veterans and their families, employees, and stakeholders.* Transition planning has included the following considerations:

- VA 5-Year Strategic Plan
- VA Reorganization
- RDCs being established
- Regional reorganization of VA
- Telecom modernization plans
- HealtheVet redesign
- Microsoft VISTA

Performance measures for IPv6 transition could include the following:

- Number and percentage of routers currently IPv6-capable
- Number and percentage of backbone network links currently IPv6-capable
- Number and percentage of network management tools (by type) currently IPv6 capable
- Number and percentage of network security tools (by type) currently IPv6 capable

Independent review(s) of IPv6 implementation project should be conducted to uncover potential lapses in prioritization among competing investments.

4.15 Risk 15 - Security

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk that pertains to the possibility that the investment does (or will) not conform to applicable Department and/or federal security standards. *Determining the level of risk are considerations of confidentiality, availability, and reliability. The risk that IPv6 security features and assurance do not comply with federal or department security standards.*	Medium	Mitigation includes laboratory testing, review of test results from other government organizations, and elimination of well known flaws as published in public sources such as the Internet. The use of sniffers and intrusion detection tools are already a part of VA's security process. Ensure IPv6-enabled technologies meet same security standards and requirements as those for IPv4 technologies. Interpretation and application of security standards regarding IPv6 characteristics and IPv4/IPv6 interactions identified during lab and production network development, testing and implementation.	IPv6-capability security gaps have been identified. Security products and technologies are being tracked as to their capability to provide an IPv4-equivalent degree of security in an IPv6 environment.	High

4.15.1 Key Considerations

The IPv6-enabled network must comply with federal and VA security standards and requirements. This security requirement is a prerequisite to operating in a production environment or even in a test environment where production data is being introduced into the network. It will be necessary to ensure that appropriate products, such as firewalls and intrusion

detection systems, are available to support an IPv6 environment. This particular risk is also a part of the assessment for Information Assurance (IA).

Additionally because IPv4 and IPv6 will be operating in a parallel, dual stack environment, any potential security interactions arising from this parallel operation must be addressed prior to activation of the IPv6 capability.

Firewall rule sets developed for IPv4 cannot be used for IPv6. This is in part because the security vulnerabilities are not the same for both protocols. This implies that security guidance for IPv6 firewalls will have to be developed in the IPv6 security community and implemented by VA security engineers who are IPv6-trained.

4.15.2 Mitigation

Methods of mitigating this risk include reviewing IPv6 transition strategies and assumptions at key points in the implementation process to make appropriate course corrections in a timely manner. The deployment team will conduct laboratory tests or utilize testing results accomplished by outside organizations, if appropriate, to provide a sufficient level of assurance that strategies and assumptions are valid. The IPv6 Transition team is also held an interagency council discussion to discuss technology advances and deployment strategies.

IPv6-capable firewall products are currently available from VA's router vendor. VA personnel have been and will continue to be trained to understand IPv6-specific security vulnerabilities and to configure the firewalls to counteract those vulnerabilities as more of the network under goes transition.

The same proactive security awareness measures that are taken with IPv4 must also be taken with IPv6. During initial IPv6 deployment, this activity will likely require parallel efforts between IPv4 and IPv6, although once IPv6 technology matures, security vulnerabilities will be focused primarily on network protocols higher in the ISO protocol stack.

Vendor security liaisons must be established that are more than a "working committee", there must be a single responsible single point of contact for all security issues and concerns.[17]

Information identified as "sensitive" in the latest inventory must be understood so appropriate mitigation of devices not IPv6-compliant can be determined and planned for.

4.16 Risk 16 - Privacy

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk that pertains to the possible violation of the legal restrictions on the collection, use, maintenance, and release of information about individuals.	Low	This issue will be tracked with the vendor and correct interoperable configurations identified, tested and implemented.	Under investigation.	Medium

[17] Carl Foster

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
	Backbone systems that currently encrypt and transmit IPv4 data may not support equivalent capabilities with IPv6				

4.16.1 Key Considerations

Direct conflict between IPv6 capability and individual privacy is not expected since IPv6 operates below the application layer where privacy is a concern. However, since security features such as encryption may be used to protect privacy, a potential conflict between IPv6 and privacy does exist. This particular risk is also being included in the assessment of Information Assurance (IA).

In the future, the following privacy concerns must be addressed:

- Individual privacy could be affected by assigning each individual an IP address which could then be used to track the individual's activities.[18] The Electronic Privacy Information Center (EPIC) points out in *IETF developed RFC 3041, "Privacy Extensions for Stateless Auto-configuration in IPv6* "This aspect of the IPv6 standard increases end user privacy by enabling users to periodically randomize their IPv6 address as well as generate temporary addresses, thus preventing the creation of a unique, unchangeable IPv6 address assigned to a specific person."

- Individual privacy could be affected unless the public were assured that VA is not collecting, maintaining, or using the IP addresses obtained from individuals accessing our websites, and public information available in general from VA, to track their movements on the Internet, instant messaging, etc.[19]

4.16.2 Mitigation

To mitigate privacy risks, the availability of security features such as encryption will be tracked with the vendor and correct interoperable configurations identified, tested and implemented.

The potential privacy issue caused by assigning each individual an IP address which could then be used to track the individual's activities could be mitigated using techniques discussed in IETF RFC 3041, "Privacy Extensions for Stateless Auto-configuration in IPv6."

Privacy concerns on the part of the general public could be mitigated by ensuring that VA is not collecting, maintaining, or using the IP addresses obtained from individuals accessing our websites, and public information available in general from VA, to track their movements on the Internet, instant messaging, etc.

[18] Comments of The Electronic Privacy Information Center (EPIC) March 8, 2004
[19] Hal Corbin, Director, VA Privacy Service; Heidi Hamzi, VA Office of E-Government, Privacy Service

4.17 Risk 17 - Project Resources

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk that pertains to the assets available or anticipated; including people, equipment, facilities and other things used to plan, implement, and maintain your project. *Insufficient quality or quantity of staff or equipment is not available when needed for IPv6 transition.*	Medium	Sufficient funding and appropriate staff resources will be made available to the IPv6 transition effort. Training of VA staff and contractors is a key element of this strategy	Government and contractor resources are being applied for the planning, transition, and testing of IPv6 capability. Training activities and related expenditures are in the planning process.	High

4.17.1 Key Considerations

As with any project, the success of the IPv6 transition project depends on the availability of resources of a type, quantity, and availability that meets project needs. VA is currently working to obtain program funding for FY 11-14.

Factors that benefit the availability of sufficient resources for IPv6 transition include the following:

- The five year time frame beginning as of FY 09 which will spread the expenditure of funds over a period of time.
- The latest VA inventory indicates that a considerable percentage of IP-aware network devices are already IPv6 compliant.
- VA will be acquiring IPv6-capable devices as part of ongoing technology refreshment.

It appears likely that the materials required to make VA backbone IPv6 capable will be available in time to meet the mandate. However, in addition to these materials, adequately trained staff and security and network management support components must be similarly available. Acquisition of the security and network management components and the adequate training or acquisition of IPv6-qualified staff remain as funding commitments that must be resolved to meet the mandate.

4.17.2 Mitigation

Sufficient funding and appropriate staff resources will be made available to the IPv6 transition effort. Training of VA staff and contractors is a key element of this strategy.

Mitigation requires identifying additional funding requirements needed to enable IPv6 capability on the backbone, modifying spending priorities, and requesting additional funding.

4.18 Risk 18 - Human Capital

Date Identified	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
April 2009	The risk that pertains to the availability of staff with required skills and experience. *Insufficient staff with required qualifications is not available when needed for IPv6 transition*	Medium	Sufficient and appropriate staff resources will be made available to the IPv6 transition effort. This will be accomplished through various types of training targeted to the different audiences. The IPv6 transition will be given sufficient priority to ensure success.	Government and contractor resources are being used for the planning, transition, and testing of IPv6 capability. Training activities over the next three years are being planned and funded.	High

4.18.1 Key Considerations

This risk is closely related to *Risk 17 - Project Resources*. Trained staff is required to deploy, configure, operate, and troubleshoot network, security and network management products. A shortfall in the availability of IPv6-capable staff presents a risk to the successful completion of the IPv6 transition project. Staffing considerations include the following:

- Types of staff needed
- Quantity of staff needed
- Types of training
- Types of staff to be trained
- Quantity of training needed

In addition to IPv6-capable staff, executives and managers must be provided with IPv6 knowledge to successfully fund and manage the effort. Procurement personnel must be included in IPv6 awareness training to ensure that newly acquired IP-aware products are IPv6 capable.

4.18.2 Mitigation

A variety of tools will be utilized to mitigate this risk. Tools such as web resources, live and recorded seminars, discussion groups newsletters and training bulletins can help inform, indoctrinate, and train VA executives, managers, procurement personnel, and technical staff to enable them to meet VA goals.

IPv6 Training combined with Risk Assessment Management following FISMA guidelines, and also IPv6 Testing, are emerging as the dominate mitigation factors with IPv6 migration. And although, these simply and primarily identify issues and conditions, the actual technical method approach selection, along with Firewall, DNS and/or DNSSEC in conjunction with IDS and IPS and the method approach of these, and the evolving Security Policies of VA, will continue expected reliability of services and provide the potential for new features to be gradually implemented across VA enterprise. Some of the topical areas address can be easily understood by content of the following website link.
http://www.verizonbusiness.com/us/about/news/displaynews.xml?newsid=23394&mode=vzlong&lang=en&width=530

4.19 Additional Risks

Although the current VA backbone has been tested as IPv6 capable, it is not too early to consider the risks that may be expected to affect VA once the backbone has been IPv6 enabled. As local area networks in VA field offices are made IPv6 capable and the protocol is adopted by user organizations, the risks will grow. As the network backbone protocols are largely transparent to users, the earlier risks are concentrated in the infrastructure categories (e.g., feasibility, reliability, technology). It is expected that considerations will trigger risk in the application layer categories (e.g., Surety, Organizational and Change Management, Business, and Privacy). As these additional risks are identified, their mitigation will be reflected in VA's IPv6 transition planning documents and activities.

The following risks are examples of those that will apply after VA backbone is IPv6 enabled:

- As VA capitalizes on IPv6 capabilities, greater use of the network may cause overloading. This would need to be addressed by redesigning the network and/or providing additional bandwidth.

- Individual privacy could be affected by assigning each individual or communication device assigned to an individual an IP address which could then be used to track the individual's activities.[20] The Electronic Privacy Information Center (EPIC) points out that IETF RFC 3041; *Privacy Extensions for Stateless Auto-configuration in IPv6* addresses this issue: "This aspect of the IPv6 standard increases end user privacy by enabling users to periodically randomize their IPv6 address as well as generate temporary addresses, thus preventing the creation of a unique, unchangeable IPv6 address assigned to a specific person."

- Individual privacy could be affected unless the public were assured that VA is not collecting, maintaining, or using the IP addresses obtained from individuals accessing our websites, and public information available in general from VA, to track their movements on the Internet, instant messaging, etc.[21]

[20] Comments of The Electronic Privacy Information Center (EPIC), March 8, 2004
[21] Hal Corbin, Director, VA Privacy Service; Heidi Hamzi, VA Office of E-Government, Privacy Service

5 Potential Applications for IPv6

It is expected that the virtually unlimited address space and better encryption available with IPv6 will have an expansive impact on the enhanced functions available to VA community in the future. IPv6 will evolve in VA over a period of several years. This evolution begins with providing IPv6 capability on the network backbone. Planning should start early to identify technologies, products and User capabilities that will become feasible once IPv6 has been enabled. Requirements and constraints on the use of IPv6 capabilities should also be identified and planned. For example, concerns for individual privacy when it becomes feasible to identify each individual with an IP address, which can then be used to track movements and activities, must be addressed early on. VA has only begun thinking about how best to exploit IPv6 capabilities.[22]

IPv6 is a protocol with potential still to be realized. While there are many perceived benefits of IPv6, the technology has not matured to the point where it is obvious how IPv6 will help VA achieve its goals.

Below are examples where IPv6 could simplify problems that are perceived as more complex with IPv4.

5.1 IPv6 as a Tool for First Responders

VA maintains facilities in regions of the country prone to natural disasters. IPv6 is an enabling technology that can help facilitate emergency responses to calls regarding hazardous materials, fires, infrastructures failures, traditional crime, and public disturbance.

A project currently under way at San Diego State University combines real-time sensor information with the needs of first responders and decision makers to quickly find, evaluate, and inter-relate complex data sets in a geospatial format.

The IPv6-based system is, in essence, an imaginary link between real spaces of one square meter and an IPv6-enabled database system which links information to specific IPv6 "Latitude and Longitude."[23] Additionally, GPS locator has practical uses and potential as well as the "always-on" feature with IPv6 to support medical first responders. Because IPv6 can provide IP addresses to trillions of sensors, all of the sensor data from a specific facility can be put together into IP systems as a simple way of organizing and retrieving information. If an IP address equals a specific sensor (camera, steam pressure, vehicle tires, fire alarm, seismic motion detector, chemical gas detectors, etc.), then the sensors can be automatically mined for information to trigger alerts in an IP environment---enabling the sensors to communicate with each other when needed, and with a server that is aggregating the information to produce an actionable situation awareness and a major tool within a decision support system.

[22] The same is true for the federal government as a whole: *Survey: Feds aren't aware of IPv6 benefits* Federal Computer Week 6 June 2005.

[23] An example of using geographic reference in defining the prefix of an IPv6 address can be found in IETF internet-draft "An IPv6 Provider-Independent Global Unicast Address Format," Tony Hain, http://www.ietf.org/internet-drafts/draft-hain-ipv6-pi-addr-09.txt and "Application and Use of the IPv6 Provider Independent Global Unicast Address Format," Tony Hain, http://www.ietf.org/internet-drafts/draft-hain-ipv6-pi-addr-use-09.txt.

By linking this sensor information to their geospatial location, this real-time information can provide extremely useful site-specific information to responders.

5.2 IPv6 as a Tool for Education and Training

A full training program at VA is provided remotely either by Computer Based Training or other form of eLearning, satellite and broadband transmission.

Conceptually, IP multicast offers the ability to efficiently distribute educational content to multiple locations and viewers. For example, multicasting enables distribution of multimedia information from one or more sources to many distributed workstations. IP multicast reduces buffering and synchronization. Because only one multicast data stream is sent out multicasting preserves bandwidth and eliminates traffic redundancy.

The design of IP multicast in IPv4 has proven challenging to implement and in many networks IP multicast simply is not enabled. The developers of IP multicast for IPv6 have attempted to simplify the design of IP multicast. It is hoped that this simplification will make it easier to deploy IP multicast across one or more networks and IP multicast will become a more viable distribution channel for educational content.

Multicasting has been used successfully already in many locations such as hotels, hospitals, university campuses, etc. VA delivers content in different ways, such as DVD, shown on VA's Knowledge Network (VA's internal satellite training system), Content Delivery Network (VA's on demand video to employees' desktops at their workstation). Consequently, a logical next step will be the delivery of content over IPv6 multicast. VA can provide live links to lectures that are delivered from remote locations for example. It is also conceivable that users will someday be able to take a training class using a Smart Phone or personal digital assistant (PDA) device.

5.3 IPv6 as a Tool for User Services

Healthcare and Pharmacy Services – The network will provide access to veterans so that they will be able to schedule appointments electronically, even using their Smart Phones or PDAs. Not only will they be able to schedule appointments, but they will also be able to provide information about their symptoms, blood pressure, temperature, and other pertinent information before arriving at the doctor's office.

The network will also provide veterans with simultaneous access to doctors and pharmacists to fill out or refill their prescriptions online.

5.4 IPv6 as a Tool for Enterprise Activities

Inventory Management Implementing RFID (Radio Frequency Identification) – At issue in inventory management is the pressure to streamline processes, survive shrinking profits, control inventory, summon up innovative communication and marketing programs, and share information in real time across store, channel, and system boundaries. Managing inventory well is vital.

Good inventory management depends upon consolidating, integrating, and analyzing massive amounts of data from many sources, such as stores, suppliers, and warehouses. Inventory

shrinkage is another problem. When inventory is lost or stolen, the cost must be added to the remaining stock, thus increasing costs.

In the near future RFID tags could be associated with IPv6 addresses to make inventories more manageable and mobile. Visualize that each RFID tag or inventory item will be identified by a globally unique IPv6 address and that the device can be tracked by this IPv6 address. The IPv6 address prefix could identify the network in which the tag or item is located and the 64-bit suffix could uniquely identify the tag/item. If the prefix is defined by geographic location, the precise latitude and longitude of the tag/item could be identified from the IPv6 address.

5.5 IPv6 as a Tool for Medical Care

Many of VA's patients are not located in close proximity to a VA hospital or clinic, yet need monitoring. Recent innovations in the world of medical technology are enabling medical staff to monitor and treat their patients from a remote location.

IPv6 can be used to provide addressing and security solutions that scale across the entire department. IPv6 can potentially provide an effectively unlimited number of globally unique addresses and the end-to-end network transparency that could enable end-to-end security, auditability and privacy.

Some real-world examples where IPv6 could be beneficial include:

Electronic Intensive Care Unit – In this application, technology that combines software, video feeds, and real-time patient information to let intensive-care specialists cover ICUs (Intensive Care Units) at a number of hospitals spread a number of miles apart, from a remote place, around the clock.

TeleMedicine – Telemedicine is the utilization of telecommunications to exchange medical information and services. Physicians can maximize their time, and provide patients with a convenient and comprehensive alternative to in-office visits, including live interaction with a specially trained medical professional. Patient data reports can be triaged and accessed via the internet. The system can clear diagnostic and evaluate real-time electrograms, surface ECGs, delivered therapies, and stored electrograms. Telemedicine is a reality today over the internet but it is expected that IPv6 will be able to deliver the same kind of information available today to a doctor's PDA.

Home Telehealth – Vital signs are monitored in the veteran's home and reported electronically to a care coordinator. This is intended to provide better patient monitoring and feedback as well as reducing costs. In home telehealth, IPv6 may provide opportunities to improve the infrastructure enabling patient monitoring and treatment.[24]

Geospatial Monitoring System – This is similar to ***Section 5.1 - IPv6 as a Tool for First Responders*** above but instead of monitoring a fire alarm, a seismic motion detector, chemical gas detectors, etc. the system will monitor the vital signs of a person then correlate it with an IPv6 latitude and longitude so that it can monitor that person no matter where he/she is.

[24] See http://vaww.va.gov/techsvc/projects/HomeTelehealth.html

In addition to the above, I believe we (VA) should take this opportunity to greatly exploit the capability of IPv6 in areas where there will be very low risks, such as:

(1) RFID tagging for inventory, tracking of anything, communications identify confirmation, and even payment transactions using ISP offering this capability.

(2) Computerized bedside patient devices which can serve in a multiple purpose device including: patient call system, direct patient viewing (interactive) with a nurse or remote direct care provider, internet for learning or interactive with the outside world, diet ordering, and this would of course serve for access to medical information by any authorized direct care provider, right at the patient bedside if desired.

(3) Cognizant interactive therapy for rehabilitation with brain injury and/or slow development and/or spinal injury.

(4) Telemedicine and video conference capability can be expanded into a wide area of specialties including: tele-dermatology, tele-dentistry, tele-radiology, tele-coding and tele-billing, electronic payment receipt, live meeting for administrative, personnel management, and for finance, ship to shore satellite link especially for VA/DoD file sharing and Electronic Health Record initiatives (also Indian Health and HHS), initial consultation on-line by progressive and knowledgeable providers of care, enhanced use and partnering of well established on-line health care firms, such as WebMD, especially on-line scheduling and possible direct interface access to select a schedule date and time by a patient using internet alone.

(5) Biometrics and embedded functions and capability with sensor technology are available now in many areas of products and services, especially pharmacy, and optometry, pathology, that also provide a real and viable opportunity to provider better, faster and more accurate care to the patient directly or indirectly.

The following hypothetical timeline illustrates how the adoption of IPv6 has transpired and could continue to occur in VA.

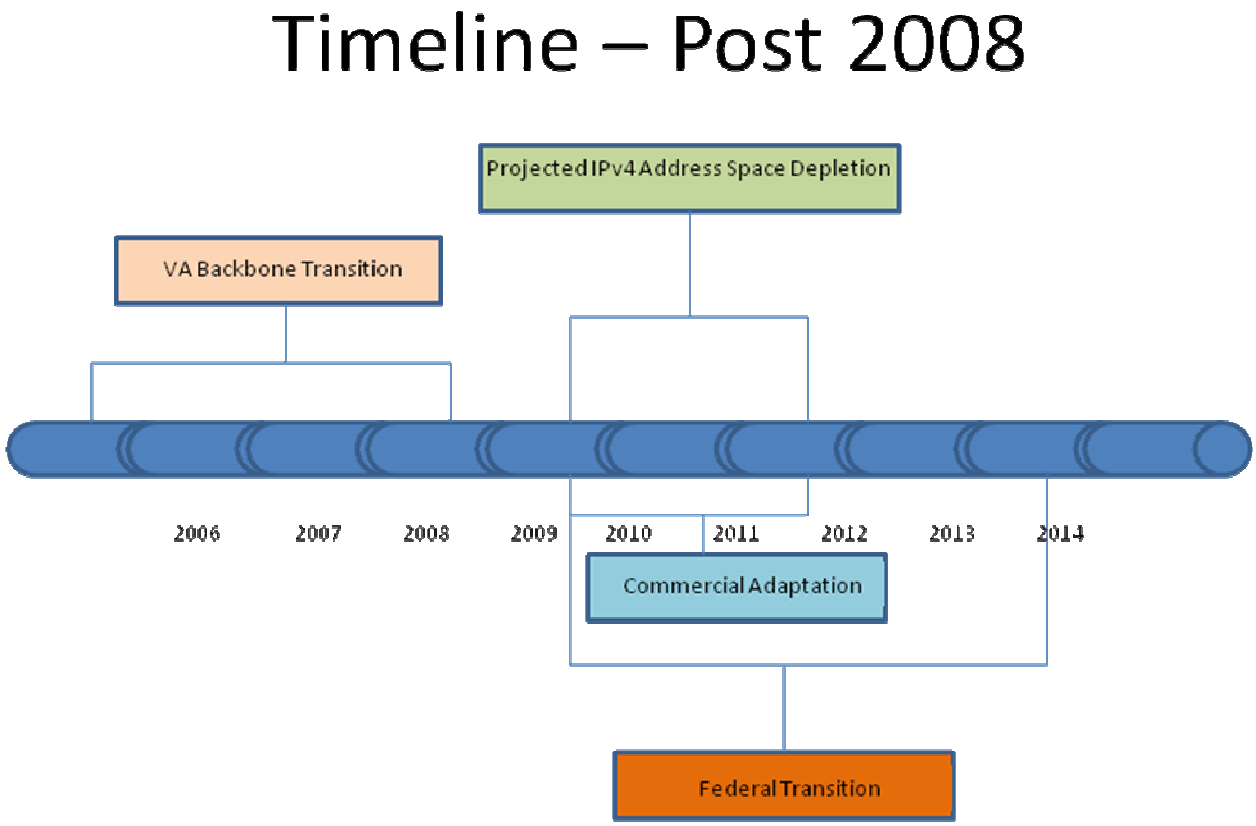


Figure 4 – Timeline - IPv6 after 2008

Appendix A – Summary of Risk Criticality

The risks addressed in ***Section 4 – Risk Analysis*** are summarized and scored on a relative rating from Non-Critical to Most Critical.

Risk Category	Probability of Occurrence[1]	Risk Impact[1]	Calculated Risk Value[2]	Evaluation Score[3]
1. Schedule	Low	Medium	2	Critical
2. Technical obsolescence	Medium	High	6	Most Critical
3. Feasibility	Low	Medium	2	Critical
4. Reliability of Systems	Medium	High	6	Most Critical
5. Dependencies and interoperability issues	Medium	High	6	Most Critical
6. Surety (Asset Protection) Considerations	Medium	Medium	4	Most Critical
7. Risk of Creating a Monopoly for Future Procurements	Low	Low	1	Non-critical
8. Capability of Agency to Manage the Investment	Low	Medium	2	Critical
9. Overall Risk of Investment Failure	Low	Medium	2	Critical
10. Organizational & Change Management	Low	Low	1	Non-critical
11. Business	Low	Medium	2	Critical
12. Data/info	Low	Medium	2	Critical
13. Technology	Medium	Medium	4	Critical
14. Strategic	Low	Medium	2	Critical
15. Security	Medium	High	6	Most Critical
16. Privacy	Low	Medium	2	Critical
17. Project Resources	Medium	High	6	Most Critical
18. Human Capital	Medium	High	6	Most Critical

[1] Low = 1, Medium = 2, High = 3
[2] Calculated Risk Value = Probability of Occurrence * Risk Impact
[3] Evaluation Score: 1 = Non-critical, 2-4 = Critical, 5-9 = Most Critical

Appendix B – Cost Details

The following table contains the Fiscal Year details of the costs which are summarized in ***Section3 – Cost Estimates***.

IPv6 Estimated Costs							
Activities	Fiscal Years						Total Cost Thru FY 2014
	FY 09	FY 10	FY 11	FY 12	FY 13	FY 14	
Transition Planning Activities	$3.5M	$3.5M					$ 7M
Training			$3M	$1.5M	$1.5M	$1.5M	$7.5M
OneVA Infrastructure & Security Equipment Refreshment							
WAN Upgrade			$15M	$15M	$15M	$15M	$60M
Security Infrastructure			$5M	$5M	$5M	$5M	$20M
Remaining Infrastructure			$5M	$5M	$5M	$5M	$20M
Pilot lab Build-out			$1M				$1M
Pilot Planning, Testing, Evaluation, Deployment			$3.075M	$3.075M	$3.075M	$3.075M	$12.3M
Operations and Maintenance			$1.78M	$1.79M	$1.79M	$1.79M	$7.15M
Total	$3.5M	$3.5M	$33.85M	$31.365M	$31.365M	$31.365M	$134.950M

Appendix C – Summary of Risks

The following table consolidates the information included under the individual risks in ***Section 4 – Risk Analysis***.

	Date Identified	Risk Category	Description of Risk ***Ipv6-Specific Consideration***	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
1	April 2009	Schedule	The risk that the project will not meet all or parts of its list of terminal elements with assigned start and finish dates, such as release(s), milestone(s), deliverable(s), or critical task(s). *This will reflect on the transition as a whole.*	Low	Sufficient funding and appropriate staff resources will be made available to the IPv6 transition effort.	Government and contractor resources are being applied for the planning, transition, and testing of IPv6 capability. Responses to a data call for an inventory of IP-aware devices have been processed. The inventory provides an indication of which devices must be upgraded or replaced to meet the June 2008 deadline.	Medium
2	April 2009	Technical Obsolescence	The risk that key technologies used in a project will lose value because a new, more functional product or technology has superseded the project's (e.g., cell phones versus the Blackberry) or when the project's product(s) become less useful or useless due to changes in other products (e.g., BETA or VHS tapes when every one has CD or DVD players) before the project has completed its full functional life-cycle. *Hardware and systems that do not support IPv6 are not replaced before they are technically obsolete.* *Purchases occur of IP-aware devices for the backbone network that are not IPv6-compliant.*	Medium	Most routers and switches that will not support IPv6 will be replaced as part of normal technology refresh processes. These were identified in VA IPv6 inventory. Some security and network management devices may need to be replaced to meet IPv6-capability requirements. Ensure that purchases of IP-aware devices for the backbone network are IPv6-compliant by June 2008.	It is expected almost all routers and switches will support IPv6 although many security and network management systems may not be ready in time. There exist methods for IP-aware devices that are not IPv6-compliant to be purchased. However, it is not expected purchases will be made that impact fulfilling the OMB mandate requirements, since these devices would not be employed in VA backbone.	High
3	April		The risk that a process, design,		Evaluate existing	IPv6 subgroups have been formed	Medium

	Date Identified	Risk Category	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
	2009	Feasibility	procedure, or plan cannot be successfully accomplished in the required time frame as proposed. *The planned IPv6 capability does not function as expected.*	Low	implementations that are similar to that being attempted by VA. Establish relations with groups, organizations, associations, vendors, and other agencies that are deploying or have successfully implemented IPv6. Ensure that technical and managerial personnel have the capability to successfully develop and implement the project. Ensure that all personnel involved with the project are properly trained in a timely manner.	for IPv6 transition. VA and contracted staff have attended IPv6 conferences and are making contacts with other IPv6 implementers. Cost estimates for training have been developed.	
4	April 2009	Reliability of Systems	The risk that the system, when operating under stated conditions will not perform its intended function acceptably for a specified period of time. *Risk that hardware and systems operating in a dual-stack IPv4/IPv6 (the likely VA IPv6 goal deployment architecture) environment are less reliable than IPv4-only systems.*	Medium	Extensive testing in a lab environment to verify reliability of dual-stack systems. Where reliability is not commensurate with that of IPv4-only systems, these issues will be investigated and where appropriate, discussed and resolved with hardware and systems vendors.	Basic testing has already occurred. More extensive testing will occur in a test environment before IPv6 is enabled on VA backbone network.	High
5	April 2009	Dependencies and Interoperability Issues	The project will fail because it depends upon the successful completion of another system or the project will not be able to work with other systems or products without an unplanned special effort. *Other organizations and vendors critical to IPv6 readiness will not support IPv6 Transition activities.*	Medium	ISPs and other organizations' networks that VA backbone network peers with will be encouraged to deploy IPv6. For the June 2008 time frame, VA backbone was dependent on being able to interoperate with other networks. Careful planning and cooperation must occur between other projects that have components that are IP-	VA is in the process of transitioning to Networx telecommunications provider services that are better able to address IPv6 interoperability. We have been in contact with several ISPs to determine their readiness. While they are not yet ready to offer public IPv6 support we continue to monitor their progress. The IPv6 PMTO will be developing	Medium

	Date Identified	Risk Category	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
			The risk that the goals of the project do not coincide with the goals of other projects.		aware.	a deployment plan to integrate other major initiatives into the overall project schedule	
6	April 2009	Surety (Asset Protection) Considerations	The risk associated with the ability of the project to meet its obligations or when there is some public or private interest which requires protection from the consequences of a contractor's default or a project's delinquency. *Key VA and/or contractor contributors default on project milestones or project work products are destroyed.*	Medium	Ongoing and frequent meetings and publication of deliverables and deliverable updates. Ensure adequate disaster recovery measures are in place.	Project conducts frequent status updates and is using existing protection mechanisms available to the project.	Medium
7	April 2009	Risk of Creating a Monopoly for Future Procurements	The risk associated with the use of closed or proprietary software/source code, as well as the dependence on a single vendor or product which in turn creates a risk that in the future the contractor will be able to reap windfall profits by charging excessive costs or reducing service quality. *Using routers from a single vendor leads to a risk of higher costs or reduced service quality because of a lack of competition.*	Low	All routers on the backbone are from a internationally recognized single vendor. However, these routers conform to standards that enable them to successfully interoperate with networks outside VA. If desired, these routers could be replaced with routers provided by other vendors; however, this would promote difficulties dealing with multiple vendors, require differing staff skills, and increase complexity in the procurement process.	VA has accepted this risk because other considerations offset risk. These include avoiding difficulties dealing with multiple vendors, reducing the type of staff skills needed, and avoiding complexity in the procurement process.	Low
8	April 2009	Capability of Agency to Manage the Investment	Risk associated with an inexperienced project owner and management team, or the lack of established OMB approved management tools, or performance indicators that show that the Department cannot deliver the project as promised. *Inability of management to manage priorities within*	Low	Assignment of experienced managers with proven monitoring and reporting tools to the IPv6 transition effort. Sufficient time will be added to schedule to allow for slippage in the schedule.	Experienced management is being applied to IPv6 transition.	Medium

	Date Identified	Risk Category	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
			resource constraints to reach the IPv6 deployment goal.				
9	April 2009	Overall Risk of Investment Failure	This risk refers to the potential that there is an inherent project weakness such as the project missing a clear link between it and the organization's key strategic priorities, including agreed measures of success. *Lack of alignment of IPv6 transition components with VA strategic IT goals, objectives, and performance measures.*	Low	Alignment of IPv6 transition with VA strategic IT goals, objectives, and performance measures. Tracking IPv6 implementation projects using relevant performance measures to control schedule, cost, and quality.	IPv6 transition is recognized and incorporated into VA Enterprise Architecture.	Medium
10	April 2009	Organizational and Change Management	Risk that activities involved in (1) defining and instilling new values, attitudes, norms, and behaviors within an organization that support new ways of doing work and overcome resistance to change; (2) building consensus among customers and stakeholders on specific changes designed to better meet their needs; and (3) planning, testing, and implementing all aspects of the transition from one organizational structure or business process to another, will not be successful. *IPv6 transition and its operation cause organizational and individual disruptions or dislocations. VA organizational changes may cause variations in the scale and nature of the project (training budget is one example).*	Low	Adjustments to the project will be made to compensate for any organizational changes.	VA has changed CIO, but the functional direction of the organization is in place. Potential IP Address Management tools are being evaluated with potential re-organization scenarios as an evaluation criteria	Low
11	April	Business	Business risk is the potential that an investment will fail to achieve the	Low	Research and testing will be conducted to verify or refute	Planning to mitigate business risk has been initiated.	Medium

	Date Identified	Risk Category	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
	2009		expectations of the project's owners and customers. *IPv6 benefits such as better security and reduced management costs are not realized.*		claimed business benefits and explore new business benefits. Steady communication of progress and tangible benefits to VA user community.	Newsletters and VA Intranet sites have been distributed or created to notify VA community of the progress and benefits of IPv6	
12	April 2009	Data/Info	Risk associated with data/information loss or disruptions caused by natural disasters (hurricanes, tornadoes, floods, earthquakes, etc.) or by area-wide disruptions of communication or electric power or malicious attacks. In addition, it can also include the ability of the investment to obtain, store, produce, share, and manipulate data as planned. *IP-aware hardware and systems that must be IPv6-capable to support the mandate are not identified in inventories.* *The process of making IP-aware devices IPv6-capable causes disruptions.*	Low	Early lab testing and production backbone network testing should identify un-inventoried IP-aware devices. These will be made IPv6-compliant, replaced or removed.	IP-aware devices in VA backbone that must support IPv6 have been inventoried and it is believed that their IPv6-compliance status has been correctly identified	Medium
13	April 2009	Technology	This risk refers to the problems associated with the use of technologies new to the Department, new software releases, or hardware new to the market. *Risk that other advanced technologies, such as data encryption and QoS, are not fully supported in conjunction with IPv6.* *Potential for unavailability of*	Medium	Identification of requirements, development of a test plan and lab testing of IPv6 used in conjunction with other advanced services will be completed.	Gaps in advanced services with IPv6 have not been evaluated extensively, although VA's preferred router/switch manufacturer is addressing gaps in their systems.	Medium

	Date Identified	Risk Category	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
			mature IPv6 technology (lack of standards). Legacy applications that cannot be upgraded or made compliant with IPv6. Inadequate supply of IPv6 ready equipment or software creates monopolistic pricing environment. *Risk that VA does not adequately define requirements for an IPv6-capable infrastructure.*				
14	April 2009	Strategic	The risk of misalignment with Department Mission and Strategic Goals, and/or the Presidents Management Agenda. *Risk that IPv6 backbone and WAN transition is not aligned with VA's strategic planning.*	Low	Alignment of IPv6 transition with VA strategic IT goals, objectives, and performance measures	IPv6 transition is recognized and incorporated into VA Enterprise Architecture.	Medium
15	April 2009	Security	The risk that pertains to the possibility that the investment does (or will) not conform to applicable Department and/or federal security standards. *Determining the level of risk are considerations of confidentiality, availability, and reliability. The risk that IPv6 security features and assurance do not comply with federal or department security standards.*	Medium	Mitigation includes laboratory testing, review of test results from other government organizations, and elimination of well known flaws as published in public sources such as the Internet. Ensure IPv6-enabled technologies meet same security standards and requirements as those for IPv4 technologies. Interpretation and application of security standards regarding IPv6 characteristics and IPv4/IPv6 interactions identified during lab and production network development, testing and implementation.	IPv6-capability security gaps have been identified. Security products and technologies are being track as to their capability to provide an IPv4-equivalent degree of security in an IPv6 environment.	High

	Date Identified	Risk Category	Description of Risk *Ipv6-Specific Consideration*	Probability of Occurrence	Strategy for Mitigation	Current Status as of the Date of this Exhibit	Risk Impact
16	April 2009	Privacy	The risk that pertains to the possible violation of the legal restrictions on the collection, use, maintenance, and release of information about individuals. *Backbone systems that currently encrypt and transmit IPv4 data may not support equivalent capabilities with IPv6.*	Low	This issue will be tracked with the vendor and correct interoperable configurations identified, tested and implemented.	Under investigation.	Medium
17	April 2009	Project Resources	The risk that pertains to the assets available or anticipated; including people, equipment, facilities and other things used to plan, implement, and maintain your project. *Insufficient quality or quantity of staff or equipment is not available when needed for IPv6 transition.*	Medium	Sufficient funding and appropriate staff resources will be made available to the IPv6 transition effort. Training of VA staff and contractors is a key element of this strategy	Government and contractor resources are being applied for the planning, transition, and testing of IPv6 capability. Training activities and related expenditures are in the planning process.	High
18	April 2009	Human Capital	The risk that pertains to the availability of staff with required skills and experience. *Insufficient staff with required qualifications is not available when needed for IPv6 transition*	Medium	Sufficient and appropriate staff resources will be made available to the IPv6 transition effort. This will be accomplished through various types of training targeted to the different audiences. The IPv6 transition will be given sufficient priority to ensure success.	Government and contractor resources are being used for the planning, transition, and testing of IPv6 capability. Training activities over the next three years are being planned and funded.	High

Appendix D – Acronyms/Abbreviations List

ACL	Access Control List
ARIN	American Registry for Internet Numbers
AS	Autonomous System
ASN	Autonomous System Number
ASM	Any source multicast
BCMA	Bar Code Mediation Administration (wireless)
BETA	Broadcasting and Education Trades Alliance (tape format)
C&A	Certification and Accreditation
CD	Compact Disk
CDCI	Corporate Data Center Integration
CIDR	Classless Inter-domain Routing Protocol
CIO	Chief Information Officer
CM	Change Management
CM	Configuration Management
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CT&E	Certification Test & Evaluation
CTO	Chief Technology Officer
D&T	Development and Testing
DAA	Designated Approving Authorities
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DNS	Domain Name Service
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice

DOL	Department of Labor
DT&E	Developmental Test & Evaluation
DVD	Digital Video Disk
EA	Enterprise Architecture
ECSIP	Enterprise Cyber Security Infrastructure Project
EOIP	Ethernet over Internet Protocol
EPIC	Electronic Privacy Information Center
ESCCB	Enterprise Security Configuration Control Board
EUD	End User Devices
FATO	Full Authority to Operate
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FTF	Federal Transition Framework
FTP	File Transfer Protocol
FY	Fiscal Year
GOTS	Government-Off-The-Shelf
GSA	General Services Administration
HR	Human Resources
HHS	Health and Human Services
IA	Information Assurance
IATO	Interim Authority to Operate
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IHS	Indian Health System
IOP	Interoperability (test and evaluation)
IOS	Internet Operating System
IP	Internet Protocol

IPAM	Internet Protocol Address Management
IPS	Intrusion Prevention System
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRD	Integrated Requirements Design
ISO	International Standard Organization
ISP	Internet Service Provider
IT	Information Technology
JITC	Joint Interoperability Test Command
LAN	Local Area Network
MAC	Media Access Control
MCSC	Managed Care Support Contractors
MHS	Military Health System
MPLS	Multi-Protocol Label Switching
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NCA	National Cemetery Administration
NIC	Network Information Center (also called Domain Name Registry)
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NSOC	National Security Operations Center
OCIS	On Call Internet Services
OEAM	Office of Enterprise Architecture Management
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
OPSEC	Operations Security
OS	Operating Systems
OSI	Open Systems Interconnection

OT&E	Operational Test and Evaluation
PCHS	Procurement of Computer Hardware and Software
PDA	Personal Digital Assistant
PII	Personal Identification Information
PM	Program Manager
PMBOK	Project Management Body of Knowledge
PMTO	Program Management Transition Office
POM	Program Objectives Memorandum
QoS	Quality of Service
RDC	Regional Data Center
RDPC	Regional Data Processing Center
RFC	Request for Comment
RFI	Request for Information
RFID	Radio Frequency Identification
RFP	Request for Proposal
RPC	Regional Processing Center
SDLC	Software Development Life Cycle
SLA	Service Level Agreements
ST&E	Security Test & Evaluation
USDA	United States Department of Agriculture
VA	Department of Veterans Affairs
VACO	Veterans Affairs Central Office
VBA	Veterans Benefits Administration
VHA	Veterans Health Administration
VHS	Video Home System (Tape Format)
VISN	Veterans Integrated Service Networks
VLAN	Virtual Local Area Network

VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network