Department of Veterans Affairs

Enterprise Architecture Guidance for the

VA IPV6 Network Transition

January 2006

Version 4.1

DOCUMENT CHANGE HISTORY

The table below identifies changes that have been incorporated into this document.

Date	Modified By	Version	Description
01/12/06	Shawn Battle	1.0	Initial Draft
01/13/2006	Al Zuech	4.1	Pre-Publication Edits

TABLE OF CONTENTS

1 Purpose 1
2 IPv6 Overview 1
3 IPv6 Resources and Relevant Documents 1
4 Current State of IPv6 2
4.1 Within Industry 2
4.2 Within Government 3
4.3 Within Veterans Affairs 3
5 IPv6 Security 4
6 IPv6 Role and Technical Architecture 4
7 IPv6 Stakeholders 4
7.1 Internal 5
7.2 External 5
8 VA Target Architecture 5
9 VA IT Portfolio Management 5
9.1 Enterprise Resource Planning (ERP) 5
9.2 Capital Planning and Investment Control (CPIC) 6
9.3 IPv6 Cost 6
10 VA Business Architecture 7
11 IPv6 Program Management 7
11.1 Program Initiation 7
11.1.1 IPv6 Impact and Risk Analysis 8
11.2 Program Planning 9
11.2.1 IPv6 Transition Plan 10
11.2.2 IPv6 Resource Plan 11
11.2.3 IPv6 Funding Plan 11
11.2.4 IPv6 Performance Plan 11
11.2.5 IPv6 Risk Mitigation Plan 12
11.2.6 IPv6 Communications Plan 12
11.3 Program Implementation 13
11.4 Program Evaluation 13
11.5 IPv6 Steering Committee/Sub-Committees 14
11.5.1 Enterprise Strategy 14
11.5.2 Transition Planning 14
11.5.3 Registry/Addressing 14
11.5.4 Training 15
12 Managing the IPv6 Transition 15
13 Major Milestones 15

LIST OF FIGURES

Figure 1. VA IPv6 Implementation Program Phases 8
Figure 2. VA IPv6 Program Plans 10
Figure 3. VA IPv6 Implementation Phase 13
Figure 4. VA IPv6 Evaluation & Alignment Phase 14

1 PURPOSE

The purpose of this document is to provide guidance to the VA stakeholders directly responsible for developing the Transition and Sequencing Plans for Internet Protocol Version 6 (IPv6). It further outlines the elements and conditions that should be considered during the development – and subsequent implementation – of the Department of Veterans Affairs (VA) IPv6 Transition Plan. This guidance which was developed by the Office of Enterprise Architecture Management (OEAM), working collaboratively with key stakeholders, is aligned with the VA Enterprise Architecture, VA Capital Planning policies and procedures, and OMB directives.

This document includes detailed discussion for program implementation, as well as strategic milestones associated with the planning and development of VA's IPv6 program. It should be noted that this document is preliminary and it is anticipated that ongoing stakeholder feedback and involvement will result in refinements to the guidance contained herein.

2 IPV6 OVERVIEW

The current version of Internet Protocol – IPv4 – was first published in 1981. While IPv4 has performed admirably over the past 25 years, the significant growth of the Internet in recent years has forced the IT community to consider the fact that the finite number of IPv4 addresses will be exhausted in our lifetime. Moreover, while a security standard exists for securing and encrypting IPv4 data packets, its use is optional and security is generally handled by proprietary security solutions.

To address the limitations of continuing to use IPv4 in the current Internet environment, the Internet Engineering Task Force (IETF) developed the protocol now commonly known as IPv6. Employing 128-bit addressing, IPv6 has been developed primarily as a mechanism for solving the shortage of IPv4 addresses that are available worldwide. However, as will be discussed later in this document, IPv6 also addresses the security-related issues that are intrinsic to IPv4.

While the United States and particularly the US Federal government, does not have an immediate concern with address depletion, and while the security plug-ins for IPv4 are generally sufficient to continue providing both short and long-term network protection, the capabilities of IPv6 will provide many advantages beyond IPv4. For example, the use of IPv6 would provide added support in the areas of infrastructure management, wireless networking and mobility, information assurance, interoperability, and convergence.

3 IPV6 RESOURCES AND RELEVANT DOCUMENTS

To better understand the nature and impact of IPv6, there has been considerable research conducted nationally and internationally, including both public and private sector business areas. Below is a list of resource documents, web pages, and artifacts used to gather information about the current and future states of IPv6, and the subsequent transition and implementation of this new protocol.

These resources include the following:

- Juniper Networks, Jan. 2006, A Guide for Federal Agencies Transitioning to IPv6
- Microsoft Corporation, *Introduction to IP Version 6*, September 2003 (updated August 2005). Available at http://download.microsoft.com/download/e/9/b/e9bd20d3-cc8d-4162-aa60-3aa3abc2b2e9/IPv6.doc
- Microsoft Corporation, *Changing to IPv6 in Windows Vista and Windows Server* (October 2005).
- The IPv6 Information Page: http://www.ipv6.org/
- The TCP/IP Guide version 3.0, (C.M. Kozierok, 2005)
- IPv6 Summit 2005, Reston Virginia: http://vaww.va.gov/oirm/telecom/ipv6/default.asp
- Internet Engineering Task Force: http://www.ietf.org/html.charters/ipv6-charter.html
- Industry for Electrical and Electronic Engineering: http://grouper.ieee.org/groups/scc32/dsrc/ip/ipv6nextgen.html
- National Institute of Standards and Technology: http://csrc.nist.gov/ipsec/
- VA Transition Planning Sub-Committee
- VA Information Technology Strategic Plan FY2002 – 2006
- VA Organizational Briefing Book, May 2005
- VA Network Design Document for Telecommunications Modernization Project (TMP)
- VA IPv6 Migration Assessment for TMP Project
- VA Infrastructure Exhibit 300
- VA Enterprise Architecture Exhibit 300
- OMB M-05-22, Transition Planning for IPv6
- OMB M-05-23, Improving IT Project Planning and Execution
- OMB Draft Memorandum 8, Nov. 15, 2005, Integrating IPv6 into Agency EA Planning
- OMB EA Framework 2.0

4 CURRENT STATE OF IPV6

4.1 Within Industry

Non-U.S. entities (notably European and Asian) have adopted the use of IPv6 more readily than the United States. This adoption has been based upon need, as the issue of IPv4 address depletion is a more significant one for non-US entities. Thus, many foreign Internet Service Providers (ISPs) have begun implementing IPv6 infrastructure networks and distributing IPv6 addresses to their customers. However, since it was developed in the United States and the US Federal government maintains control over a significant amount of IPv4 addressing capability, US IPv4 address depletion is not as great a problem today as it is in other countries.

Support for IPv6 is noticeably lacking in the Microsoft Windows operating environment. This is more of an issue within the US than in other countries since the user community outside of the US has less dependency on the Microsoft environment. Most of the hardware devices that directly support the Internet run operating systems other than Windows, (e.g., UNIX; LINUX; CISCO OS; Solaris; and OS X), so that the lack of IPv6 support within Windows will have no material impact on IPV6 implementation at the Internet backbone and distribution layers.

There are many entities in the industry (business, as well as technology) who have developed successful plans for implementing IPv6 across their infrastructure backbone. Many of the leading hardware manufactures for network equipment are prepared for a relatively smooth IPv6 and IPv4 coexistence. However, there are still a number of issues at the application level that need to be addressed regarding IPv6. Many of the physical layer elements have been resolved, but the logical layer elements and performance issues still abound. It should be noted that many of the new capabilities provided by IPv6 require cognizance of expanded IPv6 addressing at the application layer.

4.2 Within Government

OMB Memorandum M-05-22[1] established 2008 as the deadline for agencies to transition to IPv6. However, due to the current lack of an IPv6 presence across the commercial and public segments of the US technology community, the Federal government is not prepared to transition exclusively to the new protocol. After implementing IPV6, the US government must support a dual-stack IPv4/IPv6 network for years into the future. Some agencies are including IPv6 requirements in their telecommunications-related Request for Proposals (RFPs).

OMB Memorandum M-05-22 also tasked Federal agencies to begin a program assessment, which will include impact and cost analyses for transitioning to IPv6. According to OMB, this transition should be aligned with – and articulated through – the Agency's Enterprise Architecture. Subsequent research has uncovered a great number of gaps between Agency technology requirements, business requirements, and resource availability. Thus, it has reportedly been difficult to advance the implementation of IPv6. However, bridging these gaps is proving there are a larger number of individuals on both the business side and the technology side that are having difficulty bridging these gaps, with respect to IPv6 implementation. There is a possibility that the Department of Defense (which has been on the forefront of the US effort to transition to IPv6) may be putting their transition to IPv6 on hold, or at least slowing it down.[2]

4.3 Within Veterans Affairs

VA has developed an IPv6 Steering Committee, along with a number of subcommittees, to assist in the Department's transition to the new IP. The Network Infrastructure Management Team, under Information Technology Operations, has developed an IPv6 test environment, and has published an IPv6 Migration Assessment, in association with the Department's Telecommunications Modernization Project. VA has assigned an individual from the Telecommunications Operations Management team as the lead for coordinating the Department's IPv6 transition planning.

In November 2005, VA submitted its first response in compliance with M-05-22. Currently, VA is preparing to follow-up on this with its IPv6 Transition Progress Report. With assistance from VA's Office of Enterprise Architecture Management, the IPv6 Transition Team will articulate where the

[1] Karen S. Evans, Memorandum for the Chief Information Officers, August 2, 2005. Available at http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf.

[2] See, e.g., *Defense users will have to wait a little longer for IPv6*. Government Computer News, December 12, 2005. Available at http://www.gcn.com/24_34/IPv6/37737-1.html?topic=IPv6. Also see *DOD may not be ready for IPv6 transition.* Government Computer News, December 8, 2005. Available at http://www.gcn.com/vol1_no1/IPv6/37730-1.html?topic=IPv6.

Department stands regarding IPv6 Planning, Cost Analysis, Impact Analysis, Asset Control, Resource Management, and Training. Presently, the IPv6 Steering Committee and Transition Team are outlining the first draft of the Impact and Cost Analyses, which should be available for review the week of 16 January 2006.

5 IPv6 SECURITY

IPv6 incorporates the IP Security Protocol (IPsec) as an integral part of the protocol suite. IPsec was actually developed with specific IPv6 considerations in mind. These security protocols are a set of services that provide comprehensive security for IP networks, such as Authentication and Encryption of the IP datagram. Since IPv4 is the foundation of the current network, and will be for a considerable length of time, the security of IPv4 is still of significant importance to the domestic IT community. However, there are a number of security considerations that have been addressed with the new IP, that support security at the network and transport layers, but create a new set of security concerns when the need to utilize both IPv4 and IPv6 concurrently is considered.

When developing the VA's IPv6 Transition Plan, program sponsors need to consider the security implications associated with a dual stack implementation. Although IPsec is integrated with IPv6 and a plug-in for IPv4, it must still be managed properly to ensure network integrity. Moreover, since the IPv4 datagram is structured differently from the IPv6 datagram, IPsec processes the packets differently, thus creating different security parameters between the two protocols. This creates potential security issues on a dual IPv4 – IPv6 network.

The US Government will be required to maintain an IPv4/IPv6 dual-stack communications capability as long as significant IPv4-based infrastructure remains in use across the US.

6 IPv6 ROLE AND TECHNICAL ARCHITECTURE

The implementation of IPv6 is in line with VA's IT Strategic Plan and Enterprise Architecture, and also supports VA's role in National Emergency Healthcare Management. The employment of IPv6 should eliminate current impediments to communication between VA facilities and customers, emergency responders, and VA partners. The new Internet Protocol will allow VA to better implement technologies that readily support business functions across the enterprise. The Department's transition to IPv6 is a necessary factor in employing certain technologies that implement Critical Infrastructure Protection. Additional documentation about the impact of IPv6 on VA's technical architecture can be found in the VA Technical Reference Model.

7 IPv6 STAKEHOLDERS

Stakeholder involvement is essential to the success of any project. Stakeholders are those groups, teams, and individuals who are an integral part of the program's resource structure, i.e., those business and service lines, business owners, managers, and person essential to the program's success. Additionally, those who may be affected by the transition to IPv6, at any stage during the implementation, could be considered stakeholders. The development of the IPv6 transition plan should take into consideration both internal and external stakeholders. Crucial elements of stakeholder involvement include communications, resource management, product or service delivery, and the management of expectations.

7.1 Internal

The immediate list of Internal Stakeholders comprises VA's Business and Service Lines, including, but not limited to, the Offices of the Secretary and Deputy Secretary; Under Secretaries for Health, Benefits, and Memorial Affairs; and the Office of Information Technology Operations. In order to align VA's IPv6 Transition Plan with Enterprise Architecture and the Department's overall Business Plan, each of these organizations must be directly involved.

7.2 External

The VA's network and corporate enterprise is a nationwide entity, with an extensive number of touch points. Three of the direct touch points that may not be under the direct prevue of VA, but are considerably impacted by VA's network interfaces are the Department of Defense, the Internal Revenue Service, and the Social Security Administration. As VA develops its IPv6 Transition Plan, and examines the impact across the enterprise, these and other external stakeholders should be taken into consideration as well.

8 VA TARGET ARCHITECTURE

IPv6 will eventually replace IPv4 as the foundation of the Internet. The VA relies heavily on Internet-capable applications, and VA's Target Architecture reflects VA's commitment to conform to the IPv6 standard. The objective in developing the VA IPv6 Transition Plan is to assure that all VA business requirements and technology issues are addressed and satisfied, resulting in a successful IPV6 implementation.

9 VA IT PORTFOLIO MANAGEMENT

The foundation for IT Portfolio Management is the development of a single authoritative source which contains all IT related Programs, Projects, and Investments across the enterprise. Through the use of Portfolio Management, in concert with Enterprise Architecture, executives and management have the ability to evaluate every aspect, including cost and objective, of VA's Infrastructure and Technology programs, resource utilization, and the overall alignment with business objectives. The current evaluation of IPv6 transition is strategic in nature. However, this program will become operational, and will have a direct impact on operational resources. To assist in minimizing the risk to business lines and service areas, and to better ensure a qualified return on investment, each underlying element of portfolio management should be engaged, and consequently considered during IPv6 Transition development.

9.1 Enterprise Resource Planning (ERP)

While there has been significant focus in the IT industry about Voice over IP (VoIP), the broader concept of "Everything over IP" (EoIP) has begun to emerge as a likely future state of technology. Technology, applications, and devices that support IPv6 have already begun to emerge, and there are many more on the horizon. As VA examines its current IT resources, and develops plans for future procurements and upgrades, it is reasonable that the Department consider which resources are compatible with existing and emerging technology. Through Enterprise Resource Planning (ERP) VA is more readily able to plan for change across the enterprise. It is clear that IP currently touches a significant part of the network. With the continued development and deployment of the new IP it is expected that IPv6 will conceivably touch

every component on the network, thus expanding the overall scope and definition of the network. Program and resource planning in concert with business objectives and stakeholder priorities, across the enterprise, is a daunting task. As future technologies and network devices propagate across the enterprise, this task will only become more, not less, complicated. ERP is a means to logistically reduce the burden of planning, deployment, implementation, and management of IT resources, when used in a collaborative fashion with other management and performance programs. ERP is an invaluable tool, and should be a considerable component when structuring VA's IPv6 Transition Plan.

9.2 Capital Planning and Investment Control (CPIC)

The transition to IPv6 is a process that is expected to span multiple fiscal years and budget cycles. Subsequently, the IPv6 transition strategy and plan must reflect an approach that will allow continued program evaluation and reporting. The recommended mechanism for accomplishing this is through the Department's Capital Planning and Investment Control (CPIC) process. Separate program funding for the IPv6 transition has not been authorized. Funding for this initiative is expected to come through existing program dollars, by way of infrastructure improvements, and program enhancements. Future dollars for IPv6 transition and implementation should be outlined in plans submitted to OMB through the Department's Exhibit 300s; not as a separate business case, but aligned with program planning for business and strategic initiatives clearly stated within the Business Architecture.

The IPV6 Program Office should prepare an internal (component-program) Exhibit-300 budget request, for subsequent consolidation within the Department's omnibus infrastructure-support Exhibit-300 budget request, which reflects the cost, schedule and scope of the IPv6 transition.

9.3 IPv6 Cost

OMB has directed that there should be no direct funding for the transition to IPv6, therefore the cost of IPv6 program planning and implementation must be included within the normal network upgrade, augmentation, and maintenance cost categories of VA's IT infrastructure budget request. The following cost elements must be included in this budget:

VA-wide Network Planning and Design: Costs associated with project planning and network design for IPv6 Implementation.

Networking Engineering: Costs incurred to augment networks specifically to support IPv6.

Nodes and Peripherals: Costs for workstations, printers, and data storage devices etc. that are currently IPv4 capable and would eventually become IPv6 capable as well as the cost of other devices that do not current require an IP address, but may in the future.

Infrastructure Development: Those costs derived from modifications to the infrastructure based upon the configuration needs associated with the IPv6 protocol suite, versus the IPv4 protocol suite.

Application Development: Costs associated with modifying existing applications to work with the IPv6 stack, as well as the costs to develop new applications that would be impacted by the IP stack and require IPv6 specific coding.

Network Operations (O&M): Additional costs, above standard O&M, necessary to implement, manage, and maintain a dual stack IP network, or a future-centric network running the single IPv6 protocol.

Training: Costs associated with training network engineers, technicians, developers, and managers to support a dual stack network, or a future-centric network running the single IPv6 protocol as well as the cost of communicating the impact and value of the program to users, clients and other stakeholders.

10 VA BUSINESS ARCHITECTURE

The development of a convincing business case for VA's transition to IPv6 will require a detailed examination of the specific advantages that IPv6 can provide, which will also improve the efficiency and effectiveness of VA's operations and the quality of VA's service to veterans. Invariably the enhanced security, authentication with non-repudiation, and infrastructure protection capabilities, attributed to IPv6, as well as the eventual need for IPv6's extended addressability and the need to eliminate any security vulnerabilities that result from running a dual IP-stack, should be examined to achieve this purpose.

The Office of Enterprise Architecture Management will assist the IPv6 Program Office in identifying and articulating these business benefits.

11 IPV6 PROGRAM MANAGEMENT

The implementation of IPv6 is outlined in four phases: Initiation; Planning; Implementation; and Evaluation. Each phase is described in detail below. It should be noted, however, that the IPv6 Program is unique from most IT programs in that the IPv6 transition program does not include a definitive implementation cycle.

11.1 Program Initiation

The Program Initiation Phase includes the activities required to initiate IPv6 Implementation and Transition. This includes articulating and documenting Business Drivers, conducting Capability and Feasibility Studies and the establishing processes for Resource Management. Consequently, the initiation phase also incorporates the Impact and Risk Analysis, the appointment of the Program Management Team and the establishment of the IPv6 Transition Office. Each of the components necessary for establishing consistent program development through the VA Milestone Review Process and System Development Lifecycle are outlined below.

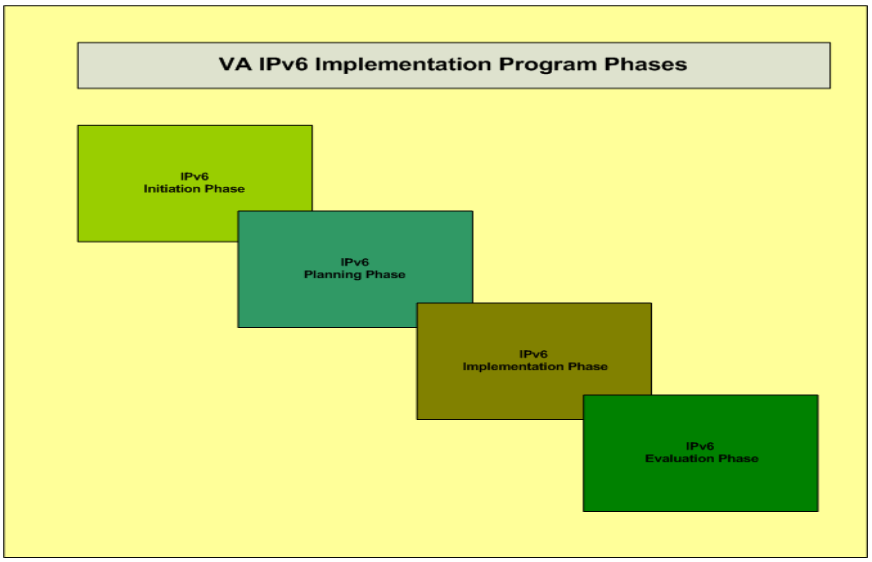

Figure 1. **VA IPv6 Implementation Program Phases**

11.1.1 IPv6 Impact and Risk Analysis

Before implementing any new program, the impact on the business must be examined, and a determination of risks and a strategy for mitigating those risks should be assessed. The impact analysis should include an assessment IPv6's capabilities and utility within the technology framework of the Department. This analysis should also examine the feasibility and reliability of the IPv6 protocol suite as a functional element that will meet the Department's business and technology needs, and the consequences associated with VA's choice to use this technology. Additionally, the analysis should at least include the following:

- A Requirements Analysis should be undertaken to determine business related rational for implementing new technology into the current systems infrastructure and business processes.

- There should be a definitive timetable for the scheduled implementation of IPv6 across the enterprise to ensure maximum functionality, and minimum disruption.

- The impact analysis and risk analysis should address the dependencies of interrelated systems across the enterprise and the subsequent affect that IPv6 implementation would have on system functionality and performance. There should be further analysis to determine the level of interoperability between the new IP version and the existing IP version, as well as any existing and emerging technologies affected by the implementation of IPv6.

- As the Department examines the impact IPv6 transition and implementation will have across the enterprise, the ability to manage the IPv6 investment must be considered. While there are no current funding dollars for this program, there must be resources allocated to operate and maintain the IPv6 environment, during transition and once it has been implemented.

- The Impact Analysis should take into consideration organizational dependencies and how changes to the environment, infrastructure, and business processes will be managed throughout the program's lifecycle.

- Technology Management is a direct consideration when assessing how IPv6 will impact the department's technical infrastructure. The IPv6 protocol suite is a technology service that potentially will impact every aspect of the department's technical infrastructure. As the department analyzes what impacts the implementation of IPv6 will have across the enterprise, preparations should be made to manage each of the technology elements subsequently affected.

- As the IPv6 program matures and begins to propagate the VA's enterprise, there are many technology elements that will be affected. One of the most significant technology elements within any system is data. Because IPv6 will affect the infrastructure, network, systems, and peripherals, enterprise wide, an analysis should be made to determine the affect this will have on data and the subsequent management of that data.

- During the planning and assessment phase of the IPv6 program, careful consideration should be given to how IPv6 compliant and capable devices are purchased. Acquisition Management is a crucial element when considering the deployment of emerging technologies. The impact analysis should address methods for assuring open competition among IPv6 vendors.

- Security and Privacy Management are essential components of the impact and risk analyses. Much of the department's information is stored on systems, and travels across the network, that is reliant upon the IP protocol suite. System security and the privacy of data should not be compromised by the implementation of new technologies or programs. The analysis should focus upon determining if the transition to IPv6 will provide equal or greater security and privacy measures. If this is not the case, then mitigation factors must be considered, and in place, prior to committing a plan of action for implementing the new protocol.

The impact and risk analysis should focus on six essential elements of Risk Management.

- Risk Threat
- Risk Criticality
- Risk Averse
- Risk Mitigation
- Risk Acceptance
- Contingency Planning

The Risk Analysis should examine alternatives and articulate which this course of action was chosen and why.

11.2 Program Planning

The Planning phase involves the creation of multiple project plans, as outlined below. These plans are created to ensure that all Program phases, activities and tasks have been clearly identified and adequate resources have been allocated. Each plan requires validation and stakeholder involvement. Figure 2 shows each of the respective plans and the sequence in which they should be completed. Each plan is described in further detail below.

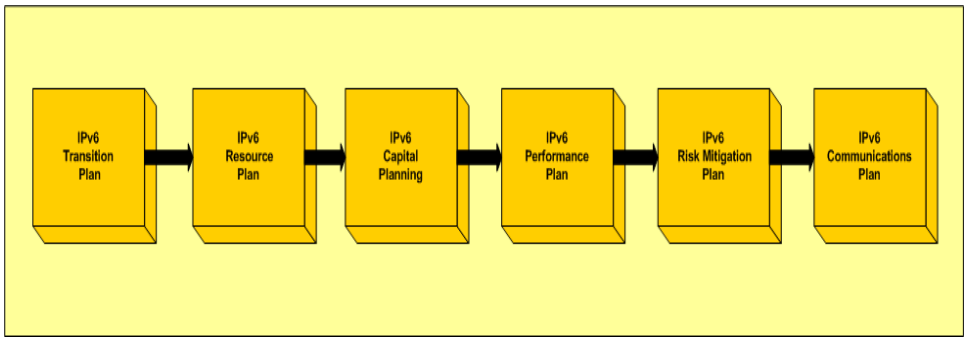

Figure 2. VA IPv6 Program Plans

11.2.1 IPv6 Transition Plan

Because all networked systems and devices in the VA currently use IPv4, the transition to IPv6 will be impacted across the enterprise. Infrastructure changes such as IPv6 should take a carefully planned and phased approach, in order to maximize success and minimize disruptions. It is important to note that OMB has stated that funding for the IPv6 transition should not be allocated as a stand-alone program. Thus, IPv6 transition planning should be considered as part of the technology refresh and infrastructure enhancement, under the auspice of O&M.

In developing a transition plan, understanding the impact of a change and subsequently addressing each potential area of impact in the transition plan is critical. Impact often has a cascading effect; failure at a particular interval and time may cause triggers that affect other program areas, or separate project within the enterprise. Therefore, it is also important to understand and address dependencies when assessing impact. Refer to section 11.1.1 for specifics on the enterprise impact of transitioning to IPv6.

The impact and dependencies of transitioning to IPv6 must then be relatively weighted and prioritized. Highest priority may be assigned to areas of greater dependency, while areas of significant impact may be awarded a lower priority to allow time to build on technical competencies. For example, existing switches and routers must be enabled to route IPv6 packets before other dependent systems and devices are configured to use IPv6; whereas transitioning the ERP system to IPv6 may be assigned a later date on the schedule.

With a thorough understanding of the impact, dependency, and priority of the IPv6 transition, a detailed technical design must be developed for each phase. Careful attention should be given to maintaining the co-existence of both the IPv4 and IPv6 environments. Each technical design should be tested and performance criteria established before it is introduced into the production environment. An iterative approach of design review, testing and release should be employed during each phase of the transition. It is important to take into consideration additional impacts and dependencies as a byproduct of the transition methodology. An iterative approach will allow for continuous defect tracking and resolution. Change Management policies and procedures should also be in place to allow for continuity of operations, and minimize any adverse impact to resources and/or service areas.

The transition plan shall include a detailed schedule listing all major tasks, subtasks, and milestones, with adequate resources assigned to every task. Dependencies among tasks shall be indicated. IPv6 transitions typically have an enterprise wide impact, which necessitates negotiation with other enterprise priority projects, resources, and stakeholders.

11.2.2 IPv6 Resource Plan

Every discreet task described and detailed in the transition plan must be properly resourced in order for it to succeed. The resource plan shall take into consideration adequate personnel to perform all the tasks, additional systems, hardware and software to execute the transition, a definitive timetable, as well as impact on all relevant enterprise resources, throughout the program's lifecycle.

Personnel resource planning is highly dependent on a sound and detailed transition plan, and shall be derived from time and tasks elaborated from the transition plan. Personnel resource identified to support the effort shall be qualified and available during the period of performance.

Tools and technology are often used in designing, developing, testing and deploying an IPv6 transition solution. Hardware, software and even professional services may be acquired in executing the transition plan. Inefficiencies are expected during the transition period, during which time IPv4 and IPv6 are expected to co-exist, and this should be taken into consideration when establishing resource allocation for the project, and included in the resource plan.

One of the business motivations for moving to IPv6 is improved service and performance over a mature network infrastructure. A natural byproduct of an IPv6 transition is expected to be greater use of the network resource, potentially impacting available bandwidth and latency. These and other potential effects of transitioning to IPv6 (such as security, network monitoring and management, network address translation, etc.) shall be identified. Resource planning for these additional uses may be forecasted, based on other potential capital plans and investments requiring or utilizing IPv6.

11.2.3 IPv6 Funding Plan

Because funding is not expressly available from OMB to specifically address the transition to IPv6, the transition shall be funded by the standard IT operations and management budget. Systems replaced as part of the standard IT refresh cycle must be IPv6 capable. Further, any new IT investments must also ensure that systems and devices are IPv6 capable.

However, because transitioning to IPv6 is effectively introducing new technology into the IT environment, justification can be made for an increase in the IT operations and management budget for training, support, and application development. Further, cost of transitioning to IPv6 can be incorporated into new capital investments requiring the availability of IPv6.

11.2.4 IPv6 Performance Plan

The performance measure for an IPv6 transition shall focus on the execution of the transition plan itself, as well as the success of the IPv6 implementation.

The performance of the execution of the transition plan may be approached from a financial perspective, comparing actual funds expended against the project's earned value. Additionally, the transition may be assessed by comparing the actual project schedule against the baseline project plan in terms of completion of tasks and meeting critical deadlines and milestones.

In assessing the performance of the IPv6 implementation, metrics may be collected with regards to help desk reports of reduced or disruption of service specifically caused by the transition. Technical performance of IPv6 may be assessed through the use of network management systems that measure packet transmission time, network packets lost or dropped over a period of time, and network latency.

Network address translation between the IPv4 and IPv6 networks may also be monitored for bottlenecks and translation efficiency.

11.2.5 IPv6 Risk Mitigation Plan

The risk mitigation plan attempts to identify events that may potentially impact the success of an IPv6 transition, and then actively manages the transition to prevent risk events while developing plans to counter the effects of a risk event, should it materialize.

A list of risk events may be developed from the impact and dependency analysis as described in section 11.1.1. In developing a risk mitigation plan, the impact of a risk event shall be stated, with a description of its potential impact to the transition or dependent stakeholders and systems. Each potential risk shall be assigned an expected level of severity; quantifying the impact to the transition should the risk event occur. In addition, it is also important to quantify the probability of the risk event occurring.

Based on the level of severity and probability of a risk event occurring, a mitigation plan shall be devised to address and/or counter the expected effects of the risk event. A mitigation plan shall describe in detail the process and procedures to be executed. The plan shall designate actor(s) who will be responsible for executing the process and procedures. A trigger shall be defined, clearly describing the condition in which a mitigation plan shall be invoked in response to a risk event. The plan shall be reviewed and concurrence obtained from all stakeholders.

11.2.6 IPv6 Communications Plan

The communication plan establishes a mechanism by which stakeholders and transition team members are kept informed of the progress and effects of the transition, support and feedback mechanism, and coordinating dependent activities.

A communications plan shall identify all transition stakeholders. Stakeholders shall be categorized based on their role and relationship to the transition, such as: business owner, decision maker, project sponsor, technical support, trainer, user, etc.

Further, a communication plan should address, in detail, the following:

- Purpose of communication

  Depending on the role and relationship, a stakeholder may expect to be informed of different aspects of the transition. It is important to channel the appropriate information to the right group of people.

- Schedule of communication

  A schedule should be devised to periodically update stakeholders of the progress or effects of the transition. Because different groups of stakeholders play a different role or have a different relationship with the transition, an appropriate schedule shall be determined and implemented.

- Condition of communication

In addition to regularly scheduled communiqués, occurrence of certain events may require special notification to stakeholders. These events should be articulated to stakeholders, including actions expected from each stakeholder as a result of these communications.

- Method of communication

  The method of communication shall also be agreed upon among the transition team and with stakeholders. Methods of communication must be effective for the purpose of the communication, in line with the severity and urgency of the subject.

Program communication is an iterative process, and must be managed and maintained throughout the life of the project. The communication plan shall be distributed and conveyed to all stakeholders, and a mechanism for feedback should be in place.

11.3 Program Implementation

This phase involves the execution of each activity and task listed in the Project Plan. While the activities and tasks are being executed, a series of management processes are undertaken to monitor and control the deliverables being output by the project. This includes the identification of changes, risks and issues, the review of deliverable quality and the measurement of each deliverable being produced against the acceptance criteria.

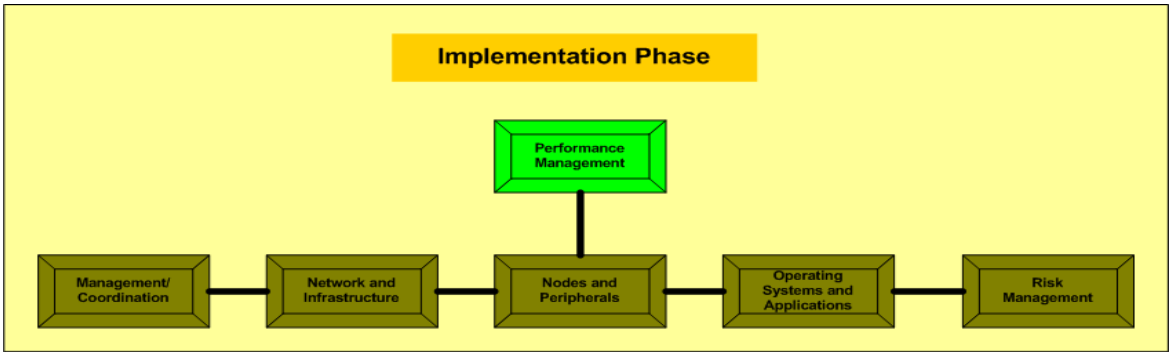

Figure 3. VA IPv6 Implementation Phase

11.4 Program Evaluation

The last remaining step is to undertake a Post Implementation Review to quantify the overall success of the project and list any lessons learnt in a formal report for future projects.

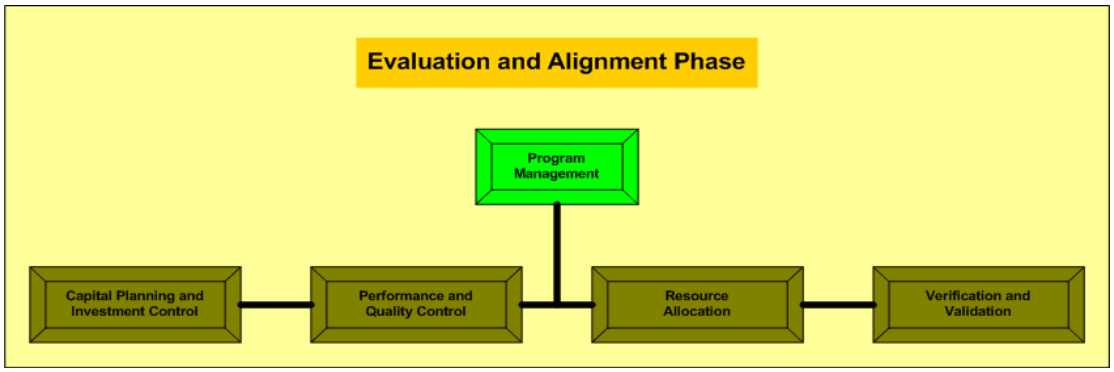

Figure 4. VA IPv6 Evaluation & Alignment Phase

- Capital Planning and Investment Control
- Performance and Quality Control
- Resource Allocation
- Verification and Validation

11.5 IPv6 Steering Committee/Sub-Committees

At this time, input from the TOM team (Valerie or Steve) is outstanding. Updates to this section will be made as information becomes available.

11.5.1 Enterprise Strategy

The Enterprise Strategy Work Group is responsible for developing the large picture related to the deployment of IPv6 for VA. The group will prepare an implementation plan that is integrated with the VA's Enterprise Architecture.

11.5.2 Transition Planning

The Transition Planning Work Group, consisting mostly of technical personnel, is responsible for developing, coordinating and implementing a cohesive transition plan for VA's migration to IPv6. Group activities shall include, at a minimum:

- Conducing a requirements analysis
- Developing and implementing a test plan for compatibility/interoperability
- Deploying a phased approach
- Maintaining and monitoring networks, and
- Updating IPv6 requirements and target architecture on an ongoing basis.

11.5.3 Registry/Addressing

The IP Registry/Addressing Work Group is responsible for evaluating IP addressing needs for VA's IPv6 transition. The group will prepare a document describing the allocation scheme for distribution of the new addresses across the Department, including the preparation of the required justifications for ARIN (American Registry for Internet Numbers) approval.

11.5.4 Training

The Training Work Group is responsible for evaluating, developing and implementing training approaches and programs for VA's IPv6 transition stakeholders (managers, staff, and technical personnel). The group will produce a document which lays out the how, when, why and who for the rollout of the entire integrated training program.

12 MANAGING THE IPV6 TRANSITION

The phased approach to IPv6 transition and implementation requires consistent monitoring and management throughout the life of the program. The implementation of IPv6 is not constructed as an overnight replacement for IPv4. It is expected that each version of IP will run concurrently for some time. Many of the devices that are IP dependent will be required to run both IP stacks at sometime during their lifecycle. Consequently, managing the IPv6 transition requires an iterative and phased approach that provides for the phase-out of IPv4 and the phase-in of IPv6. The IPv6 Transition Plan should be developed with this in mind, while also considering the impact and risks associated with managing these overlapping technologies.

13 MAJOR MILESTONES

As the VA IPv6 Transition Planning Sub-Committee begins to establish an initial plan for transitioning the Department to the new Internet Protocol, they have developed their first milestone checklist. This was presented to the group and discussed as a preliminary set. There is currently a gap between the Telecommunications Operations Management team (TOM), the Transition Subcommittee, and OEAM. However, this gap will be addressed very early in 2006 through a coordinated effort between OEAM and TOM.

In the interim, the initial milestones put forward by the Transition Subcommittee are:

- Transition Approach
- Security Plan
- Document Change Management Process
- Develop Contingency Plan
- Plan Rollout (Transition) Schedule

OEAM is recommending the IPv6 transition milestones listed below. Subsequent versions of this document will provide greater detail regarding each milestone.

<u>Initiation Phase/Strategy</u>

It should be noted that VA's IPv6 Initiation Phase is already underway.

- VA Enterprise Architecture Integration/IPv6 Business Alignment
- Creation of IPv6 Transition Office
  - Mission
  - Governance
  - Committees and Sub-committees
  - Budget
  - Acquisition Management

- Resource Management
- Standard
- Operations
- Systems
- Integration

Planning Phase

- IPv6 Architecture
- Requirements
  - Government and Industry Standards
  - Technical Guidance
  - Network Engineering
  - Application Development
  - COTS Availability
  - Acquisition
  - Policy and Procedures
  - Artifacts and Repository
- Test and Evaluation
- Transition Management
- Transition Integration
- Transition Support
- Network Solutions
- Application Solutions
- Enterprise Services
- Enterprise Management
- Information Assurance
- Training and Operational Support

Implementation Phase

The Implementation Phase for IPv6 is a uniquely iterative process.

- Management/Coordination
- Network and Infrastructure
- Nodes and Peripherals
- Operating Systems and Applications
- Testing and Validation
- Risk Management

Evaluation Phase

Because of the ongoing implementation cycle associated with IPv6, program evaluation and IPv6 performance determinations should be structured to reflect this

- Drivers/Critical Success Factors
- Resource Allocation
- Cost
- Performance

Program Analysis and Control

The IPv6 Program should be managed and analyzed:

- Iterative Processes
  - Needs Analysis
  - Functional Analysis
  - Design Synthesis
  - Integration
- Verification and Validation
- Best Practices
- Lessons Learned
- Program Realignment