IPv6 Transition Guidance

Issued by
Federal CIO Council Architecture and Infrastructure Committee

February 2006

Table of Contents

1 Introduction

Internet Protocol (IP) is the "language" and set of rules computers use to talk to each other over the Internet. The existing protocol supporting the Internet today - Internet Protocol Version 4 (IPv4) - provides the world with only 4 billion IP addresses, inherently limiting the number of devices that can be given a unique, globally routable address on the Internet. The emergence of IPv6, providing the world with an exponentially larger number of available IP addresses, is essential to the continued growth of the Internet and development of new applications leveraging mobile Internet connectivity. Although the information technology (IT) community has come up with workarounds for this shortage in the IPv4 environment, IPv6 is the true long-term solution to this problem.

Federal government agencies should prepare for the future of networking and Internet technology by enabling their networks to support IPv6 addresses and data packets. There are many considerations when introducing any emerging technology into an organization's infrastructure. Therefore, this type of transition should be done methodically and mindfully, with full awareness of the benefits, challenges, and caveats surrounding the technical implementation of IPv6. This document outlines many of these benefits, challenges, and caveats, and provides Federal government agencies with IPv6 transition "best practices" which can be used to inform agency IPv6 transition planning and the adoption of IPv6 into their IT infrastructure.

1.1 Background

In August of 2005, the Office of Management Budget issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)", establishing the goal of enabling all Federal government agency network backbones to support the next generation of the Internet Protocol Version 6 (IPv6) by June 30, 2008.

The memorandum requires the agency's network backbone to be ready to transmit both IPv4 and IPv6 traffic, and support IPv4 and IPv6 addresses, by June 30, 2008. Agencies must be able to demonstrate they can perform <u>at least</u> the following functions, without compromising IPv4 capability or network security:

- Transmit IPv6 traffic from the Internet and external peers, through the network backbone (core), to the LAN.
- Transmit IPv6 traffic from the LAN, through the network backbone (core), out to the Internet and external peers.
- Transmit IPv6 traffic from the LAN, through the network backbone (core), to another LAN (or another node on the same LAN).

The requirements for June 30, 2008 are for the network backbone (core) only. IPv6 does not actually have to be operationally enabled (i.e. turned on) by June 30, 2008. However, network backbones must be ready to pass IPv6 traffic and support IPv6 addresses. Applications, peripherals, and other IT assets which are not leveraged in the execution of

the functions mentioned above are not required for the June 30, 2008 deadline. Agencies are expected to verify this new capability through testing activities. They are also required to maintain security during and after adoption of IPv6.

In support of these goals, OMB Memorandum 05-22 identifies several key milestones and requirements for all Federal government agencies. These requirements are:

- By November 15, 2005
  - Identify an IPv6 agency lead
  - Complete inventory of IP-aware hardware devices in network backbone
- By February 28, 2006
  - Develop a network backbone transition plan for IPv6
  - Complete an IPv6 progress report
- By June 30, 2006
  - Complete inventory of IP-aware applications and peripherals with dependencies on network backbone
  - Complete an IPv6 transition impact analysis
- By June 30, 2008
  - Complete network backbone transition to IPv6

All agencies are required to submit these deliverables to OMB on or before these due dates. Requirements for Enterprise Architecture submissions are described in Chapter 3 of this document.

The memorandum (05-22) indicated the CIO Council Architecture and Infrastructure Committee (AIC) would publish transition planning guidance. Subsequent to the release of OMB M-05-22, the AIC published three "chapters" of IPv6 transition planning guidance. The first chapter, published on November 15, 2005, addressed the use of Enterprise Architecture (EA) to plan for enterprise-wide IPv6 transition. This chapter also included instructions to agencies on how to submit their IPv6-related artifacts with their February 28, 2006 Enterprise Architecture assessment. The second chapter discussed some of the more technical elements of agency transition, such as 1) IPv6 transition planning best practices; 2) networking & infrastructure; 3) addressing; 4) information assurance; 5) pilots, testing and demonstrations; 6) applications; 7) standards; and 8) training. The third chapter discussed IPv6 transition governance. It described the management structure of the Government-wide IPv6 transition effort, as well as the roles and responsibilities of each of the agencies and organizations involved (e.g. OMB, CIO Council, large and small agencies). The second and third chapters of transition guidance were provided to agencies on February 2, 2006. They were sent directly via e-mail to agency IPv6 leads. Agency leads were given an opportunity to comment on the guidance.

This document is a compilation of these three chapters of guidance, incorporating the feedback received from agencies.

The AIC will be publishing an additional chapter of guidance, which discusses acquisition and procurement of IPv6-capable/ready assets. Once this chapter is released, it will be sent to agencies for comment, and subsequently incorporated into this document. This document will also be updated periodically as new best practices are identified and as otherwise deemed necessary by the CIO Council Architecture and Infrastructure Committee (AIC). Recommendations for updating the content of this document will be provided by the AIC IPv6 Working Group as new transition strategies are identified based on lessons learned.

1.2   *Purpose & Scope*

This document provides additional guidance on how to implement the requirements of OMB Memorandum 05-22. It includes:

- An overview of IPv6 features, benefits, and implementation challenges
- Guidance for agencies incorporating IPv6 into their enterprise architecture
- Instructions for Enterprise Architecture submissions due to OMB
- Recommendations and best practices for IPv6 enterprise transformation planning
- A description of the Governance process and roles and responsibilities

1.3   *Document Organization*

This document is composed of five chapters: Introduction, IPv6 Overview, Integrating IPv6 into the Enterprise Architecture, Understanding Key Transition Elements, and Governance.

The first chapter, *Introduction*, provides background information and discusses purpose and scope.

The second chapter, *IPv6 Overview*, provides a background on the emergence of IPv6, and an explanation of the features, benefits, and challenges of introducing IPv6 into the networking environment.

The third chapter, *Integrating IPv6 into Enterprise Architecture Planning*, describes the process for integrating IPv6 into the agencies strategic planning and enterprise architecture activities. This chapter also discusses key EA deliverables.

The fourth chapter, *Understanding Key Transition Elements,* provides detailed "best practices" and recommendations in several of the most critical aspects of IPv6 transition. These areas are those relevant to a Federal government agency introducing IPv6 into their network environment. These areas are:
- Networking Infrastructure
- Address Planning
- Information Security
- Transition Mechanisms
- Standards
- Training

   o Testing
   o Cost of Transition

Chapter 4 also outlines the suggested content areas for an IPv6 transition plan. Agencies may use the content areas included in this section to shape their own IPv6 transition plans.

The fifth chapter, *Governance*, details the governance processes supporting the Federal government transition from IPv4 to IPv6.

2   IPv6 Overview

IPv6 is the next generation protocol for the Internet, designed to support continued Internet growth in number of users and functionality. The current version, IPv4, was developed in the 1970's and provides the basis for today's Internet interoperability. IPv4 suffers some limitations that may be inhibitors to growth of the Internet, and use of the Internet as a global networking solution.

IPv4 allows for as many as 2^{32} (4,294,967,296) addresses. Although this seems like a very large number, it is much too small for tomorrow's Internet. Considering the population of the Earth is approximately 6.6 billion people, with IPv4 we can not even afford to give a single IP address to every person on the Earth.

IPv6 has been under development by the Internet community for over ten years and is designed to overcome these limitations by greatly expanding available IP address space, and by incorporating features such as end-to-end security, mobile communications, quality of service, and system management burden reduction.

The emergence of the Internet as a fundamental technology for commercial and social activity has been most apparent since the creation of the World Wide Web in the early 90's. The Internet has grown rapidly in the past five years, to a scale well beyond that which the original Internet designers envisioned over twenty years ago.

Without sufficient global IP address space, applications are forced to work with mechanisms that provide local addressing. In the interim, there have been numerous optional "workarounds" (such as Network Address Translation) and extensions to IPv4 to try to overcome its limitations. Network Address Translation (NAT) allows multiple devices to use local private addresses within an enterprise while sharing one or more global IPv4 addresses for external communications. While NAT has to some extent delayed the exhaustion on IPv4 address space for the short term, it complicates general application bi-directional communication. IPv6 eases the complexity of providing end-to-end security. IPv6 removes the common motivation for the use of NAT since global addresses will be widely available.

The true transition of the global Internet from IPv4 to IPv6 is expected to span many years. During this period of transition, many organizations introducing IPv6 into their infrastructure will operate in a dual-stack environment supporting IPv4 and IPv6 concurrently, possibly for the foreseeable future.

There is not a one-size fits all transition strategy for IPv6. The incremental, phased approach allows for a significant period where IPv4 and IPv6 can co-exist using one or more transition mechanisms to ensure interoperability between the two protocol suites.

2.1 IPv6 Features and Benefits

The evolution of the IPv6 protocol represents the work of many different Internet Engineering Task Force (IETF) proposals and working groups, and represents several years of effort. IPv6 was designed to build on the existing features of IPv4 and provide new services and capabilities. The rationale is to:

- Extend the IP address space enough to offer a unique IP address to any device.
- Enable stateless IP auto-configuration and improved "plug and play" support
- Provide support for network address renumbering.
- Enable mandatory implementation of IP Security (IPsec) support for all fully IPv6-compliant.
- Improve support for IP Mobility.

Listed below is an overview of several features and benefits IPv6 is intended to provide.

- **Larger address space** – IPv6 increases the IP address size from 32 bits to 128 bits. Increasing the size of the address field increases number of unique IP addresses from approximately 4,300,000,000 (4.3×10^9) to 340,282,366,920,938,463,463,374,607,431,768,211,456 (3.4×10^{38}). Increasing the address space to 128 bits provides the following additional potential benefits:
    - o **Enhanced applications functionality** – Simplifies direct peer-to-peer applications and networking by providing a unique address to each device.
    - o **End-to-end transparency** – The increased number of available addresses reduce the need to use address translation technologies
    - o **Hierarchical addressing** – The hierarchical addressing scheme provides for address summarization and aggregation. These approaches simplify routing and manage routing table growth.
    - o **Auto-configuration** – Clients using IPv4 addresses use the Dynamic Host Configuration Protocol (DHCP) server to establish an address each time they log into a network. This address assignment process is called stateful auto-configuration. IPv6 supports a revised DHCPv6 protocol that supports stateful auto-configuration, and supports stateless auto-configuration of nodes. Stateless auto-configuration does not require a DHCP server to obtain addresses. Stateless auto-configuration uses router advertisements to create a unique address. This creates a "plug-and-play" environment, simplifying address management and administration. IPv6 also allows automatic address configuration and reconfiguration. This

capability allows administrators to re-number network addresses without accessing all clients.
   o **Scalability of multicast routing** – IPv6 provides a much larger pool of multicast addresses with multiple scoping options.

2.2 IPv6 Challenges

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

2.2.1   Maintaining interoperability and security during transition

Agencies will need to maintain network interoperability as they transition away from today's IPv4-only environment. During the initial phases of transition, agencies are likely to move to an environment to accommodate native IPv6 and encapsulated IPv6, in a largely IPv4 network leading to a ubiquitous dual-stack environment. As applications transition and the use of IPv4 diminishes, agencies will operate in an environment largely as an IPv6 network. Hardware and software interoperability will be essential as agencies move forward with their IPv6 plans and interconnect their networks across dual environments. Since maintaining interoperability and security for these types of evolving environments is the highest priority, the transition period should be kept minimized.

There are many possible combinations of technical IPv6 transition strategies. There are also a number of transition mechanisms (e.g. dual-stack, tunneling, translation) which agencies can choose from with more emerging from the technical community. The introduction of IPv6 on an enterprise scale will introduce a number of challenges including scalability, integration, and security. In the near term, there is concern about creating vulnerabilities in existing IPv4 networks by deploying IPv6 and its transition mechanisms. This risk can be mitigated by development of an overall phased approach to IPv6 network transition which addresses end-to-end interoperability, performance, and security issues. Agencies may also want to consider controlling the use of IPv6 on IPv4 networks that carry classified traffic until the networks carrying unclassified traffic have been successfully transitioned and tested. An integrated and coherent strategy should be developed to allow IPv4 and IPv6 to operate on these networks using emerging IPv6 security products. Furthermore, in many cases, there will be an on-going need for interaction with IPv4 enclaves outside of the agency requiring transition mechanisms to be planned accordingly.

2.2.2   IPv6 Standards and Product Evolution

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

3   Integrating IPv6 into Enterprise Architecture Planning

IPv6 is an enterprise transformation driven by business, environmental, and technology factors, the scope and impact of which extend well beyond the IT organization. Since IPv6 has the potential to impact agency decisions about business performance, business processes, information, technology infrastructure, security and other strategic initiatives, IPv6 should be incorporated within the agency's strategic planning and enterprise architecture (EA) development activities.

3.1   Agency Responsibilities

To appropriately address the requirements in OMB Memorandum 05-22, related to agencies' enterprise architecture submissions to OMB in February 2006, agencies should:

- ✓ Incorporate IPv6 into their IRM Strategic Plan,
- ✓ Update their enterprise architecture, including:
  - o The baseline architecture
  - o The target architecture
  - o The transition strategy
  - o Other enterprise architecture documentation, as necessary,
- ✓ Complete their IPv6 transition plan, and
- ✓ Complete their IPv6 progress report.

Only scorecard agencies are required to provide enterprise architecture submissions. For other, non-scorecard agencies, OMB will be looking at their IPv6 Transition Plan and IPv6 Progress Report. For guidance on developing an IPv6 Transition Plan, refer to Chapter 4 (Transition Elements). Additionally, while small agencies are not required to submit enterprise architecture plans, they can still benefit from the guidance provided in this chapter.

Agencies should create a cross-functional team to support IPv6 transition planning and implementation, including representatives from agency lines of business, infrastructure, application development, security, enterprise architecture, capital planning, and procurement. The IPv6 team should remain actively engaged with agency leadership through all phases of the transformation effort.

3.1.1   IRM Strategic Plan

Implementing IPv6 represents a strategic opportunity for agencies to provide improved services with greater efficiency. Several benefits were discussed in Chapter 2 of this document.

The first step to incorporating the benefits of IPv6 into the agency's strategic and EA planning processes should be to incorporate IPv6 as a strategic initiative within the agency's Information Resource Management Strategic Plan. The IRM plan documents the agency's strategic goals for IRM over a multi-year horizon and aligns them to the agency's overall strategic plan as required by OMB Circular A-130 (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf).

In particular, agencies should identify:

- **Strategic drivers for the adoption of IPv6 by the agency.** Agencies should link IPv6 to specific strategic goals and objectives for the agency. For example, IPv6 may advance agency goals associated with expanding electronic government, improving services to citizens, or other goals specific to each agency's mission.
- **How IPv6 could benefit agency lines of business.** Agencies should identify which programs and lines of business will achieve improved performance through IPv6 adoption. Moreover, IPv6 may enable the agency to provide additional services to citizens, businesses, or other organizations.
- **How IPv6 could benefit cross or multi – agency lines of business**. Agencies should identify programs and lines of business which will achieve improved performance or strategic advantage through IPv6 adoption. For example, IPv6 may be a key enabler for improving communications infrastructure for first responders.
- **The impact IPv6 adoption will have** on other enterprise activities such as organizational planning, budgeting, procurement and human resources management
- **Performance objectives** for the IPv6 transition program itself. Creating meaningful performance metrics for IPv6 deployment is a cornerstone of effective transition planning and will enable agency business owners to see the return the IPv6 business case represents.

3.1.2   Updating the Enterprise Architecture

Per OMB Circular A-130, agencies are required to have three primary elements within their enterprise architectures: a baseline (as-is) architecture, a target (to-be) architecture, and a transition strategy that defines the process of migrating from the baseline to the target architecture. IPv6 should be incorporated into each of these perspectives of the agency enterprise architecture.

The baseline architecture should include IT assets affected by IPv6 transition as per the IP device and technology inventories required by OMB Memorandum 05-22. The target architecture should reflect not only the impact on agency networking components, but should also reflect the impact of IPv6 on other architectural views such as Business, Strategy and Performance, Data, Service Component, Technology, and Security and Privacy. The agency's IPv6 transition plan should be consistent with the EA transition strategy.

3.1.2.1   Baseline Architecture

OMB Memorandum 05-22 requires agencies to perform an inventory of their existing IT infrastructure to determine which assets will be affected by the transition of the network backbone to IPv6. The initial inventory to be completed by November 15, 2005 must list networking hardware within the backbone. The second inventory to be completed by June 30, 2006, is much broader and should include not only networking hardware, but

applications, operating systems, and other devices impacted by the transition of the network backbone to IPv6.

Agencies should utilize the inventory data to update the current technology and service component views of their baseline architecture, specifically:

- The **Service Component** architectural view should be updated to incorporate IP dependency information for agency IT assets. Assets which depend on IP (but are not IPv6 compliant) can be identified directly from the architecture and prioritized accordingly within the agency's capital planning activities.
- The **Technology** architectural view should be updated to reflect which technology assets within the agency either provide or require IP services, and whether those assets, such as routers and servers, are capable of being upgraded to support IPv6.

3.1.2.2   Target Architecture

IPv6 represents a common technology standard for all federal agencies. As such, it should be incorporated as an element of the agency's target architecture for 2008 and beyond. However, the effect of the transition to IPv6 extends well beyond the selection of agency networking components. The agency's target architecture should reflect the impact of IPv6 within all architectural views, specifically:

- The **Strategy and Performance** architectural view should reflect the fact that IPv6 will represent a strategic change within the agency, as documented in the agency's IRM Strategic Plan. Specifically, the target EA should document:
  - o Strategic drivers for the adoption of IPv6 which will include compliance elements such as Memorandum 05-22, but more importantly, business opportunities to improve services and efficiency
  - o Changes to the agency's IRM strategic goals and objectives
  - o Performance measurement indicators for the IPv6 transition initiative, aligned to the FEA Performance Reference Model
- The **Business** architectural view should be updated to incorporate changes to the agency's business and investment activities resulting from IPv6 adoption, specifically:
  - o New or modified lines of business for the agency that will be enabled through IPv6 adoption, including cross-agency initiatives; these agency lines of business should be aligned to the FEA Business Reference Model
  - o Dependencies and impacts of IPv6 adoption on agency programs
  - o Changes to the agency's IT investment portfolio; this will include not only the IPv6 transition initiative itself, but other investments that will realize new risks, benefits and costs from the transition to IPv6
- The **Data** view may or may not be affected, depending on the scope of the agency's data architecture. Specific issues to consider include:
  - o IP address representation. IPv6 addresses differ both in structure and in length from IPv4 addresses. Agencies that currently record IP

addresses within data resources may need to modify their data schemas accordingly.

- The **Service Component** view of the architecture should clearly document changes to agency IT services and applications that will result from IPv6 adoption. The target should include:
  - o Additional agency IT services that will be enabled through IPv6 adoption
  - o Service and application dependencies on specific versions of IP
  - o Changes to the agency applications portfolio necessitated by IPv6 adoption
- The **Technology** view of the architecture should be updated to address:
  - o Changes to technology standards. IPv6 is not a single published standard but rather a collection of Internet Engineering Task Force specifications, known as Request For Comment (RFC) documents. Agencies should clearly define an IPv6 compliance standard for their agency that may incorporate a subset of RFC features as required.
  - o Changes to additional technology infrastructure and standards necessitated by the need for IPv4/IPv6 interoperability, such as translation gateways, tunneling mechanisms and others
  - o Changes to technology hardware and software products
  - o Changes to the agency networking topology, if the agency technology architecture extends to this level of detail
- **Security and Privacy** may be represented as a cross-cutting concern rather than a separate view of the target architecture. IPv6 deployment within the network backbone may have a substantial impact on the target security architecture, including:
  - o Changes to network security standards and configuration as a result of the IPv6 end-to-end security model
  - o Changes to IT security policy
  - o Privacy considerations

3.1.2.3   EA Transition Strategy

OMB Memorandum 05-22 requires agencies to develop an IPv6 transition plan, and provide the completed plan as part of the February 2006 EA assessment submission to OMB. Although all agencies are expected to develop a detailed IPv6 transition plan as part of their regular project management activities, scorecard agencies do not need to include this particular document as part of their February 2006 EA assessment.

For scorecard agencies, OMB will be reviewing agency EA Transition Strategies in order to gauge progress towards the June 30, 2008 deadline. Agencies should submit their EA Transition Strategy document as part of the February 2006 EA assessment. Agency EA Transition Strategies should reflect IPv6 key activities, timelines, milestones, and dependencies.

IPv6 will require careful attention to several specific transition strategy analysis activities, including:

- **Detailed dependency analysis and sequence planning.** Dependency on a specific version of IP may be widespread and require research and testing on the part of agencies. The successful transition of an IT service to be IPv6-capable includes not only the networking hardware, but might also include workstation and server operating systems, applications, and peripheral devices. These "ripple effects" must be effectively documented within the agency target architecture if the transition is to succeed. This analysis is a critical input to the development of a sequencing plan that organizes all of the major elements of IPv6 deployment as subprojects within the larger initiative.
- **Interrelationships with other infrastructure programs.** The adoption of IPv6 within the agency network backbone is a major initiative that will have far-reaching consequences for agency EA transition planning. IPv6 adoption should not be treated as an isolated initiative, but should be carefully coordinated with other agency modernization initiatives, such as lines of business outsourcing, HSPD-12, COOP, and RFID,
- **Ensuring the transition strategy drives IT investment decisions.** Agencies should use their transition strategy as a basis for making future IT investment decisions, including ensuring IT investments appropriately address agency IPv6 requirements.
- **Establishment of quarterly performance milestones.** The transition strategy should incorporate specific quarterly performance milestones for IPv6 adoption. These may include elements such as address allocation, hardware deployment, and the completion of user training. Problems with IPv6 adoption can then be identified early in the transition so managers can make course corrections and develop risk mitigation strategies as appropriate.

Agencies should refer to the OMB EA Assessment Framework Version 2.0 (issued in November 2005) for more detailed information on the components of an effective EA Transition Strategy.

3.1.2.4 Other EA Documentation

With the release of the OMB EA Assessment Framework Version 2.0, OMB will evaluate whether and how the EA is actually being used within the agency to achieve results. As a result, the revised Framework incorporates a number of new assessment criteria to evaluate agency performance. There is specific policy-alignment criteria for IPv6, which clearly identify the documentation and activities required to achieve a specific maturity level. However, IPv6 adoption will also play a substantive role in assessing agency maturity levels for several other assessment criteria, namely:

- **EA Governance and Management**: Governance is the mechanism by which EA planning decisions are realized and enforced within the agency. Therefore, agencies should be prepared to provide governance charters, agendas, minutes and other documentation to demonstrate that:

- o The agency body responsible for EA governance is aware of the requirement for IPv6 transition and the specific role IPv6 plays within the agency's target architecture;
- o The agency body charged with implementing IPv6 is coordinating its activities with the EA governing body, and changes to either EA or IPv6 implementation policies are effectively communicated to each group;
- o The EA provides agency managers with the ability to observe the current state of the IPv6 transition within the agency and its impact on other strategic agency initiatives
- **CPIC Integration:** The EA should drive the selection, control and evaluation of agency investments and other capital planning activities. To achieve this goal, agencies should be prepared to provide evidence through their CPIC guides, business cases and investment review board minutes that:
  - o IPv6 compliance is clearly established as a requirement within the agency's procurement and investment review guidelines
  - o The agency EA is capable of reporting which agency investments are included in the IPv6 implementation within the agency network backbone
- **Business Driven:** Agencies should be able to clearly establish a line of sight between the agency's strategic planning activities and the IPv6 implementation, specifically:
  - o IPv6 transition planning is clearly identified as a major initiative within the agency's EA Program Plan;
  - o The strategic drivers supporting IPv6 adoption identified within the agency IRM Strategic Plan are clearly documented within the agency's target strategy and performance view
  - o Performance measures associated with IPv6 implementation are clearly documented within the agency's target strategy and performance view and are organized using appropriate measurement indicators identified within the FEA Performance Reference Model
- **Business Process and Service Improvement:** Agencies should leverage the analysis they performed as part of the IRM Strategic Plan to document the business benefits they expect to achieve through IPv6 implementation, specifically:
  - o Agency lines of business that are expected to attain service improvement or cost savings as a result of IPv6 implementation
  - o New or modified lines of business and agency programs enabled through IPv6 technologies
  - o Expected impact on agency programs as a result of IPv6 implementation
- **IT Implementation Improvement:** Agencies should be able to demonstrate that their IPv6 transition strategy is directly integrated into their methodology for implementing agency IT projects. Specific evidence should include:
  - o Guidance to IT projects (whether custom-developed or COTS) identifying specific technical requirements for IPv6 compliance
  - o Documenting the impact of IPv6 adoption on the agency's plans to establish a service-oriented architecture infrastructure

3.1.3   IPv6 Progress Report

The IPv6 progress report should include the following:

- ✓ Status of the second IP devices and technologies inventory (Attachment A of OMB Memorandum 05-22),
- ✓ Status of the IPv6 impact analysis (Attachment B of OMB Memorandum 05-22), and
- ✓ Overall agency progress towards June 30, 2008 IPv6 transition target date

Agencies should include interim milestones and dates in the progress report for each of the deadlines specified by OMB Memorandum 05-22. These milestones should align with those included in the agency IPv6 transition plan and EA transition strategy.

Agencies should also include any challenges, issues, or risks they are facing with completion of the second inventory, impact analysis, or other aspects of the agency's transition to IPv6.

Subsequent to the February 2006 EA assessment, OMB will continue to monitor the progress of agency IPv6 efforts through the standard, quarterly EA assessments and provide feedback to the agencies as appropriate. The OMB Enterprise Architecture Assessment Framework Version 2.0, and the agency EA Transition Strategy, will be used to assess agency progress.

3.1.4   Submission to OMB

Scorecard agencies are to provide the following information to the FEA PMO (via email at fea@omb.eop.gov) as a part of their standard February 28, 2006 EA submission:

- Agency EA Assessment using Version 2.0 of the OMB Enterprise Architecture Assessment Framework,
- A complete inventory listing of all EA documentation used to complete the February 28, 2005 Assessment,
- A copy of all your agency's current EA program documents and artifacts, including a copy of the IRM Strategic Plan and EA Transition Strategy, and
- A copy of your agency's IPv6 progress report

Non-scorecard agencies are to provide the following to OMB (via email ipv6@omb.eop.gov) by February 28, 2006:

- IPv6 Transition Plan
- IPv6 Progress Report

Following the initial February 28, 2006 submission, agencies must submit quarterly IPv6 status reports, showing progress against previously established milestones, and updated transition plans (or EA Transition Strategies), on day 60 of each quarter. These quarterly reviews will begin in FY 2006 Q3, and correspond with the review schedule established

for other OMB initiatives, such as E-Gov Implementation Plan Scorecard assessments and EA assessments. To ensure progress is being monitored throughout the transition period, agencies are required to submit these materials to OMB through the earlier of the quarter ending June 30, 2008 or the completion of the agency's network backbone transition.

Agencies which have an EA should submit their Enterprise Architecture Transition Strategy and IPv6 Progress Report with each of their quarterly reviews. These agencies should be prepared to provide their IPv6 Transition Plan for supporting documentation, if requested by OMB. Agencies which do not have an Enterprise Architecture should submit their IPv6 Transition Plan and Progress Report with each of their quarterly reviews.

4   Transition Elements

Since IPv6 is the "next generation" Internet protocol and introduces new standards, agencies are faced with the challenge of limited IPv6 transition "success stories" on which to model their enterprise transformation strategy. This chapter is a compilation of existing recommendations and best practices around IPv6 enterprise transformation planning, gathered from the experiences of public sector organizations (particularly the Department of Defense), the private sector, and the Internet research and development community (such as the North American IPv6 Task Force).

The intended audience of this chapter includes the individuals responsible for development of agency IPv6 transition plans, such as agency IPv6 program leads, chief architects, and other technologists working in IPv6 transition or future maintenance of the IPv4/IPv6 environment. Both agencies providing their own network services and those purchasing services from a provider are required to develop a transition plan. Agencies purchasing network services are expected to work closely with the provider in developing the transition plan and monitoring the status of plan activities.

This chapter presents a discussion of:

- Best practices and recommendations for:
    - o Identifying Networking Infrastructure Requirements
    - o Identifying Address Planning Requirements
    - o Identifying Information Security Requirements
    - o Identifying Transition Mechanisms Requirements
    - o Identifying Testing Requirements
    - o Identifying Standards Requirements
    - o Identifying Training Requirements
    - o Identifying Transition Costs
- Components of an effective IPv6 transition strategy

Due to the varied business and technical environments of Federal government agencies there is not a "one size fits all" IPv6 transition plan template. Therefore, the content of this chapter is not intended to be prescriptive or directive. However, agencies may use the information provided as a guide for development of their IPv6 transition strategy.

4.1   Understanding Key Transition Elements

There is a set of key transition elements which agencies should consider as they adopt and begin to deploy IPv6. The initial considerations for transition are as follows.

4.1.1   Identify Networking Infrastructure

One of the initial activities agencies should undergo is an assessment and identification of their existing network infrastructure. Each agency should review their overall networking infrastructure and perform an inventory assessment. This was a requirement of OMB Memorandum M-05-22. The result of this analysis will provide agencies with an initial template of those components required for transition to IPv6. In addition to performing a raw inventory of assets, there are other ways for agencies to think about their current architecture which can assist agencies with requirements gathering, and determination of the most appropriate transition plan for the agency.

The first of these activities is to categorize the type of transition that is going to be executed. Appendix B lists three "typical" IPv6 transition scenarios. This is not an exhaustive set of scenarios, but a base set of general cases from which to work. Once an agency determines which scenario most closely aligns with their environment, the caveats listed will provide a sense of the transition requirements which require consideration in the development of a transition plan.

4.1.2   Identify an Addressing Plan and Request Addresses

Prior to requesting IPv6 addresses, each agency should determine the IPv6 address space it will require over the next five year period. Once that is determined then the agency can request an IPv6 address assignment for deployment either from the American Registry for Internet Numbers (ARIN) or their Internet Service Provider, as appropriate. Additionally, agencies can review IETF RFC 3513 IPv6 Addressing Architecture (ftp://ftp.rfc-editor.org/in-notes/rfc3513.txt) and IETF RFC 3587 IPv6 Global Unicast Address Format (ftp://ftp.rfc-editor.org/in-notes/rfc3587.txt) to develop an understanding of the IPv6 Addressing Architecture in general.

Each agency will need to define the network topology and hierarchy of their network and whether mobility is to be part of the long term deployment of IPv6. As such, the following questions will need to be answered:

- Number of External Networks to be accessed from within the agency and means of access to Service Providers
- Number of Local Area Networks within the agency
- Number of devices, nodes, and in general number of networked entities that will be assigned IPv6 Addresses

- Whether seamless mobility must be supported on the agency's internal network as well as remote mobility over external networks
- Definition of multicast communications and affected networks
- Transition strategy for migrating current IPv4 network to IPv6; IPv4/IPv6 interoperability plans, and expected rate of transition

Once this information is identified, an agency will be able to architect its IPv6 address routing topology to support their core infrastructure and the edges of their network. Subsequent address assignment to local area networks will also be possible. The addressing plan should consider a clear and concise mapping of the addresses to the networks physical topology.   Schemes used to combine or aggregate the data should maximize efficiency of the administrators' network.

Developing an addressing plan is an individual organizational effort for each agency and needs to be planned considering the operational requirements, transition strategy, and network infrastructure components within each agency's network of operations. Identifying the various management components for an addressing plan is an important part of performing this exercise because the architectural choices involving aggregation of the address space can make the management of the network more efficient. Some of the management considerations to examine when defining an addressing plan are as follows:

- Management and allocation of IPv6 addresses on the network
- Management of routing protocols to be used across the network
- Management of devices, nodes, etc., to use IPv6 stateful or stateless auto-configuration
- Management and allocation of the IPv6 resource information
- Management of DNS domain names to IPv6 addresses and the reverse
- Management of Internet Services on the network
- Management of IPv4/IPv6 transition and interoperability services

How do I request IPv6 addresses if my agency provides its own Internet Services?

Federal agencies performing operations as an Internet Service Provider (ISP) are the only agencies that need to acquire IPv6 address space from the ARIN. Most agencies that perform as an ISP already have a Registry Service Agreement (RSA) in place for their IPv4 address allocations so there should be few modifications required to institute an RSA for the IPv6 allocation. An Address Allocation template is located at http://www.arin.net/registration/templates/index.html. It is important to note that the minimum allocation size is /32. If agencies have questions with respect to the requirements, they may contact the National Telecommunications and Information Administration (NTIA) or the General Services Administration (GSA) for assistance. (Please refer to Appendix A for contact information.)

What if my agency receives Internet Services from a provider?

Federal agencies that receive their Internet services via an Internet Service Provider (ISP), telecommunications provider, or the GSA Federal Technology Service will acquire their IPv6 address space from their ISP. Agencies should be in contact with their service provider to address this issue as soon as possible and to ensure the provider is fully aware the federal government is transitioning to IPv6. The address plan will need to address the origin of the contracted IP service and the availability of IPv6 service offerings for your physical location. Transition plans need to address change in provided services or a change in the service providers that may offer additional IP services.

4.1.3   Identify Information Security Plan

Agencies are required to conduct risk assessments and develop security plans in accordance with the Federal Information Security Management Act (FISMA) and as required by National Security Policy, OMB Policy, and in accordance NIST standards and guidance as necessary.

Several security implications of adopting IPv6 within an agency are provided below as initial guidance to identify a network security infrastructure plan within each agency.

- Security applications infrastructure currently used on an IPv4 network will need to be replicated, with an expectation that the same level of assurance is provided in the IPv6 network. Examples of those applications are Intrusion Detection, Firewalls, Network Management of IP Packets, Virus Detection, Intrusion Prevention, Secure Web Services Functions, etc.
- If end-to-end IPsec security is to be implemented, there will be a need to identify PKI, key management, and policy management infrastructures that meet the scalability and security verification requirements for intra-network communications (e.g. nodes, devices, and sensors).
- If end-to-end IPsec security is implemented, the current network perimeter security infrastructure applications (e.g., firewalls, intrusion detection systems) that depend on accessing and viewing IP transport data payloads must be aware that they will not be able to view that part of the IP packet and alternate mechanisms should be deployed.
- If VPN tunnels are used to encapsulate IPv4 within IPv6, or IPv6 within IPv4 as a transition method for deployment:
  - o The tunnel endpoints between the VPN should be secured as the traffic transits the VPN.
  - o When an encapsulated IPv6 packet enters or leaves the VPN and Intrusion Detection is required, it should be understood that the Intrusion Detection application or other network security method used to permit a packet on that network, has been ported to IPv6, as previously identified.
- Wireless network access from IPv6 nodes require in depth security analysis for implementation when stateless auto-configuration is used, in addition to current

methods to secure IPv4 wireless networks.
- Seamless Mobility with IPv6 will need to support the required security as identified by the agency to permit secure access to the network whether across the internal network, or remote from an external network.
- IPv6 on a network should not be turned on by default unless all network security infrastructures are implemented. (Note that some products may have IPv6 enabled out-of-the-box.)

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

4.1.4   Identify Transition Mechanisms

The objective of this section is to identify the different transition mechanisms options available to an agency while planning its adoption of IPv6. These mechanisms are intended to ensure interoperability between IPv4 and IPv6 and can categorized in the following three broad classes: dual-stack, tunnels, and translation mechanisms. For a description of these technical mechanisms, please refer to Appendix C.

In order to identify the best suited transition mechanisms for an agency, it is recommended that the agency have an in-depth up-to-date understanding of its current IT environment. This understanding will help choose the best suited transition mechanisms. It is important to note that one size does not fit all. While selecting a mechanism the key objective should be to reduce the impact on the existing environment. It should also be noted that an agency does not have to only use one transition mechanism, but can select multiple transition mechanisms as best fits their deployment needs.

When selecting a transition mechanism one must consider the functionality required, its scalability characteristic, and the security implications of each mechanism. It is also important to request that IPv6 products comply with the requirements, and to monitor CERTS alerts as the introduction of new IPv6 features and software code could lead to vulnerabilities. Also, domain name system (DNS) servers must support IPv6 resource records.

4.1.5   Identify Network Testing Strategy

Before an agency deploys IPv6 it is important to test IPv6 for the network. In some cases cross-agency collaboration for IPv6 testing of implementations will reduce the effort for testing, but each agency will need to identify their specific network testing requirements. In addition, agencies can work with industry to test their network access and some of the IPv6 features that require wide-area-network testing. One of the existing industry IPv6

network pilots is the Moonv6 www.moonv6.org network. The AIC CIO IPv6 Working Group members will work together to determine test strategies.

4.1.6   Identify Standards

The Office of Management and Budget, CIO Council AIC IPv6 Working Group, and NIST will work together to identify the standards to be used within the Federal government. In the interim, it is suggested that agencies become familiar with the IEFT web site; the IETF (www.ietf.org) defines Internet Protocol Standards.

4.1.7   Identify Training Needs

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

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

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

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

Specialized – As IPv6 deployment advances and the base level of understanding become more pervasive, the need for specialized training will emerge. This type of training should focus less on IPv6 specifically and address greater technological topics where IPv6 plays an important role. An excellent example would be the area of Mobility. Projects such as MetroNet6 (http://www.cav6tf.org/html/metronet6.html), focus on utilizing IPv6 and Mobility concepts for improved communication systems for first responders. Course work in this area would cover not only Mobile IPv6, but also topics such as MANET, NEMO, mobility-specific security issues, access media, and possibly low bandwidth compression algorithms.

The Federal CIO Council AIC IPv6 Working Group will work in conjunction with agencies, industry, and OMB to identify specific agency training needs and potential solutions.

4.1.8   Identify Cost of Transition

Transition costs will stem from several sources, but will likely come from software and hardware, training, application porting, consulting services, and operational costs.

IPv6 is to be phased into the agencies' infrastructure and applications through their lifecycle management processes. Agencies are expected to acquire IPv6 capability while upgrading infrastructure as part of the normal technology amortization/replacement lifecycle. The availability of transition mechanisms will allow agencies to replace only that equipment deemed necessary to facilitate IPv6 integration. As equipment is replaced with newer equipment, native IPv6 capability will be part of the equipment's basic operating capability. Consequently, the cost of transition from equipment replacement should be significantly minimized.

Training will be an important part of the integration process. Agencies will potentially need to make plans for training their staff. The specific cost of training each person will depend upon the role they play in the integration process.

While the June 30, 2008 deliverable applies only to transitioning the network backbones to support IPv6, some agencies may decide to begin migrating applications (e.g. enterprise applications other than those that support network operations) prior to or following June 2008. Costs for porting applications will vary on the complexity of the port, the size of the application (measured by lines of code), and what, if any, new features are being architected into the application.

Professional services will be another cost of integration. These professional services may come in the form of transition planning assistance, development of a test plan, deployment assistance, and/or help desk support. Regardless of the type of services acquired, professional services are likely to be a component of any agency's transition costs.

Finally, agencies will incur operational costs as they begin making their network backbones IPv6-ready so they are positioned to leverage the benefits of IPv6.

4.2   Components of an IPv6 Transition Plan

The following is a list of components that could be used as the basis for an IPv6 transition plan. Although agencies are not required to include all of these components in their transition plan, it is recommended that agencies cross-check their own plan against this list to ensure no critical transition elements have been overlooked.

1. Identification of strategic business objectives
2. Identification of transition priorities
3. Identification of transition activities
4. Transition milestones
5. Transition criteria for legacy, upgraded, and new capabilities
6. Means for adjudicating claims that an asset should not transition in prescribed timeframes
7. Technical strategy and selection of transition mechanisms to support IPv4/IPv6 interoperability
8. Management and assignment of resources for transition
9. Maintenance of interoperability and security during transition
10. Use of IPv6 standards and products
11. Support for IPv4 infrastructure during and after 2008 IPv6 network backbone deployment
12. Application migration (if required to support backbone transition)
13. Costs not covered by technology refresh
14. Transition governance
    a. Policy
    b. Roles and responsibilities
    c. Management structure
    d. Performance measurement
    e. Reporting
15. Acquisition and procurement
16. Training
17. Testing

5   Governance

Planning and execution of the government-wide adoption of IPv6 requires close coordination and cooperation among all of federal agencies, departments, and organizations. This section discusses the IPv6 management structure and roles and responsibilities of agencies and other entities, to include:

- Establishment of an IPv6 Advisory Group to support, advise and inform OMB;
- Establishment of an interagency IPv6 Working Group, under the purview of the CIO Council, to escalate and address critical implementation issues on a continuing basis;
- Ongoing and open communication between OMB, the Federal CIO Council, and agencies through formal and informal channels;

- Sponsorship of inter-agency forums to share transition planning best practices, challenges, and experiences;
- Instantiation of an IPv6 collaboration and information sharing work space on CORE.gov;
- Acquisition of IPv6 address-space;
- Implementation of common IPv6 acquisition and procurement policy, through the Federal Acquisition Regulations (FAR); and
- Issuance of IPv6 standards and guidance by the National Institute of Standards and Technology (NIST) as necessary.

OMB will issue additional policy or guidance, as needed. Federal government agencies are responsible for executing the policy/guidance provided. OMB will evaluate agencies' status through existing budgetary and acquisition review processes. As the transition to IPv6 proceeds, the need for additional IPv6-focused entities will be continually evaluated.

This chapter is composed of two sections: Management Structure and Roles and Responsibilities. The first section, *Management Structure*, identifies the Federal government agencies (and other entities) involved in IPv6 transition oversight and execution, and outlines the relationships between these organizations for the purposes of oversight, reporting, and implementation. The second section, *Roles and Responsibilities,* further defines the role of each organization identified in the management structure.

5.1   *Management Structure*

The Federal government has the unique challenge of implementing IPv6 with a "one enterprise" approach in an environment where agencies have historically operated as independent, autonomous entities. Therefore, a management structure for this IPv6 transition like must provide adequate controls, oversight, and support for common solutions, while still enabling agencies to develop transition plans and solutions that best fit their unique environment. The following management structure has been developed to address these needs.
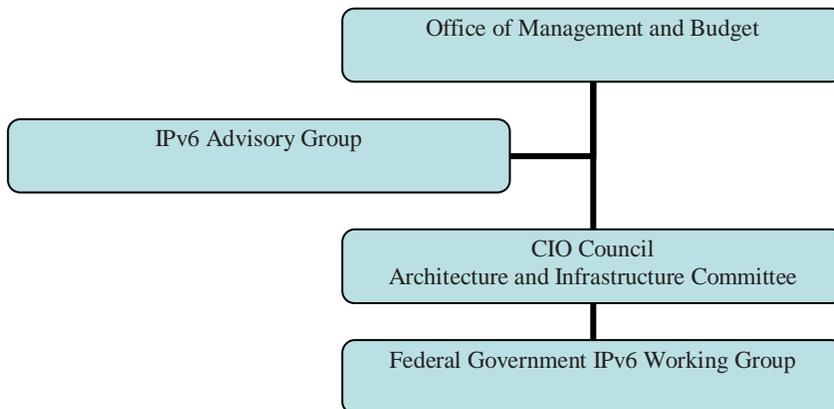
5.2   Roles and Responsibilities

The following list of responsibilities is focused on ensuring that all critical aspects of IPv6 transitioning are addressed in a timely fashion consistent with the already existing roles and missions of the agencies. It is not intended to redefine, reallocate, or otherwise alter existing agency roles and missions.

5.2.1   Office of Management and Budget

OMB is responsible for oversight of the government-wide transition to IPv6. OMB will assess agency progress and compliance with Memorandum 05-22 through the FEA PMO quarterly enterprise architecture review process. As required, OMB will report to Congress on the Federal government's progress with IPv6 transition.

As needed, OMB will establish government-wide policy for IPv6 implementation, including consultations with General Services Administration (GSA) to implement Federal government IPv6 acquisition policy.

OMB will also engage the support of an IPv6 Advisory Group throughout the transition process to inform and assist in execution of IPv6-related management and oversight activities.

5.2.2   IPv6 Advisory Group

An IPv6 Advisory Group has been established and is comprised of selected subject matter experts and other Federal government resources. This group will serve as an IPv6 advisory group to OMB leadership throughout the transition, and will provide information on current market trends and transition best practices related to IPv6. The IPv6 Advisory Group consists of subject matter experts and will be expanded as needed to ensure appropriate representation of the following functions:

- IPv4/IPv6 transition
- Cybersecurity and personal privacy
- Technology standards
- Acquisition and procurement
- IP address acquisition and management
- Network management and testing

The IPv6 Advisory Group is assisting OMB with execution of IPv6 oversight activities, including (but not limited to) development of IPv6 guidance, coordination and documentation of common processes and procedures related to IPv6 transition, communication with agencies, and facilitation of public forums.

5.2.3   CIO Council Architecture and Infrastructure Committee

The AIC of the CIO Council has selected John McManus, Deputy CIO and CTO of NASA as the IPv6 lead. This individual serves as chair of the IPv6 Working Group and functions as the primary Working Group liaison to OMB.

Per OMB Memorandum 05-22, the CIO Council has published IPv6 transition guidance to Federal government agencies and additional guidance will developed as necessary. The CIO Council will distribute this guidance to agencies via e-mail, and will post all guidance documents on the public CIO Council web site (www.cio.gov) and OMB E-Gov web site (www.whitehouse.gov/omb.egov).

Additionally, the AIC will assist OMB in communicating Federal government IPv6 policies, documents, and related information to agency IPv6 leads (primarily though the Federal CIO Council e-mail list-servs and Core.gov).

5.2.4   IPv6 Working Group

An IPv6 Working Group was established in February 2006, and will operate, at a minimum, until the completion of the network backbone transition from IPv4 to IPv6.

The IPv6 Working Group is comprised of all agency IPv6 leads, and other subject matter experts (as determined and requested by the membership of the group). The IPv6 Working Group will also charter sub-working groups focusing on several functional areas relevant to Federal government IPv6 transition, as necessary. Some of the functional areas include (but are not limited to):

- Standards
- Cybersecurity
- Testing
- Address Allocation and Management
- Acquisition

The IPv6 Working Group Chair is responsible for communicating directly with agency IPv6 leads regarding membership, and will facilitate all meetings of the Working Group. The Chair is responsible for regularly reporting status to OMB. The Group is responsible for developing and documenting plans, such as a charter, mission, vision, goals, action plan, etc. The IPv6 agency leads are also responsible for communicating IPv6 requirements to their agencies and serve as a primary IPv6 point of contact for their agencies.

5.2.5   Agencies

As per OMB Memorandum M-05-22, all large and small Federal government agencies are responsible for ensuring that IPv6 data packets can be successfully transmitted on their network backbones by June 30, 2008, while maintaining interoperability with all other components of their IT infrastructure. Agencies are also responsible for ensuring continuity of operations and security of all networks and systems, throughout the IPv6 transition.

Agencies must comply with the requirements of Memorandum M-05-22, as clarified by IPv6 guidance published by the CIO Council.

In addition to the requirements established in Memorandum M-05-22 (i.e. submission of first IP-device inventory, IPv6 transition plan, status report, second IP-device inventory, and impact analysis), agencies must also submit quarterly IPv6 status reports, showing progress against previously established milestones, and updated transition plans (or EA Transition Strategies), on day 60 of each quarter. These quarterly reviews will begin in FY 2006 Q3, and correspond with the review schedule established for other OMB initiatives, such as E-Gov Implementation Plan Scorecard assessments and EA assessments. To ensure progress is being monitored throughout the transition period, agencies are required to submit these IPv6 materials to OMB through the earlier of the quarter ending June 30, 2008, or the completion of the agency's network backbone transition.

Agencies which have an EA should submit their Enterprise Architecture Transition Strategy and IPv6 Progress Report with each of their quarterly reviews. These agencies should be prepared to provide their IPv6 Transition Plan for supporting documentation, if requested by OMB. Agencies which do not have an Enterprise Architecture should submit their IPv6 Transition Plan and Progress Report with each of their quarterly reviews. More detailed information about these requirements is included in Chapter 3 (Integrating IPv6 into Agency Enterprise Architecture Planning) of this document.

Scorecard agencies are to provide the following information to OMB, with their EA assessment materials, via email to fea@omb.eop.gov. Non-scorecard agencies are to provide their information to OMB via email to ipv6@omb.eop.gov.

It is also strongly recommended that all agency IPv6 leads participate in the interagency IPv6 Working Group. In order to ensure interoperability amongst Federal government agencies and take advantage of best practices, agencies are encouraged (where deemed appropriate by the agency) to leverage solutions recommended by the IPv6 Working Group.

5.2.6   Other Agency Responsibilities

In addition to the above responsibilities, the following agencies have responsibilities.

5.2.6.1   National Institute of Standards and Technology (NIST)

As the Federal government technical standards-making body, NIST will work with OMB and the IPv6 Working Group to evaluate the need for common standards and technical guidance.

NIST will work with stakeholders to ensure any standards/guidance developed is in alignment with existing industry standards and is in the best interest of the Federal government. Furthermore, NIST will provide the IPv6 Advisory Group and OMB with

additional guidance as necessary and maintain representation on the IPv6 Advisory Board.

5.2.6.2   National Telecommunications and Information Administration (NTIA)

To help facilitate the address space acquisition process, NTIA, within the Department of Commerce, will assist OMB in its role as the central point of coordination in advising agencies requiring guidance as they proceed with identifying their IPv6 requirements. NTIA will also facilitate and assist agencies, as necessary, as they interface with ARIN. (For information on acquiring IPv6 addresses, refer to Section 4.1.2 of this document.)

NTIA will provide guidance in a manner which reinforces Federal government cyber-security policy and best practices. NTIA will also maintain representation on the IPv6 Advisory Board.

5.2.6.3 General Services Administration (GSA)

GSA will update the Federal Acquisition Regulation (FAR), as deemed necessary by the FAR Council, for the acquisition of IPv6-capable assets and services. The FAR will reference the acquisition requirements. GSA will also assist OMB, as necessary, with developing an acquisition strategy to support the network backbone transition.

The Core.gov portal (www.core.gov) will be used as the primary Federal government site for interagency IPv6 collaboration and information sharing. GSA will initiate the IPv6 information sharing site on Core.gov, for use by the IPv6 Working Group and other individuals involved in the transition. GSA will be responsible for ensuring individuals have proper instructions for registering and using the site, and will facilitate a Core.gov training session for all agency IPv6 leads. The Core.gov team will respond to agency inquiries about the site. GSA will also ensure this site has the appropriate level of security and access control. GSA and the Core.gov team will work with the IPv6 Working Group throughout this process.

Additionally, GSA will maintain representation on the IPv6 Advisory Board and provide support for cross-agency initiatives related to IPv6 throughout the transition period.

Appendix A: Points of Contact

Listed below are the primary points of contact for the organizations listed in this document, as it relates to Federal government IPv6 transition.

OMB General IPv6 Inquiries
IPv6@omb.eop.gov

OMB
Carol Bales
Senior Policy Analyst
carol_bales@omb.eop.gov
(202) 395-9915

IPv6 Working Group
John McManus
Deputy CIO and CTO, NASA
Chair, IPv6 Working Group, CIO Council AIC
jmcmanus@nasa.gov
(202) 358-1802

National Telecommunications and Information Administration
Cathy Handley
chandley@ntia.doc.gov
(202) 482-0012

National Institute of Standards and Technology
Doug Montgomery
Advanced Network Technologies Division
dougm@nist.gov
(301) 975-3630

Sheila Frankel
Senior Computer Scientist
Computer Security Division
Sheila.Frankel@nist.gov
(301) 975-3297

General Services Administration
Lee Ellis
lee.ellis@gsa.gov
(202) 501-0282

Appendix B: Transition Scenarios

This appendix lists three "typical" IPv6 transition scenarios. This is not an exhaustive set of scenarios, but a base set of general cases from which to work. Once an agency determines which scenario most closely aligns with their environment, the caveats listed will provide a sense of the transition requirements which require consideration in the development of a transition plan.

Scenario 1:   Wide-scale/total dual-stack deployment of IPv4 and IPv6 capable hosts and network infrastructure. Agency with an existing IPv4 network wishes to deploy IPv6 in conjunction with their IPv4 network.

- Assumptions: The current IPv4 network infrastructure [1] has an equivalent capability in IPv6.

- Caveats: Do not disrupt existing IPv4 network infrastructure assumptions with IPv6. IPv6 should be equivalent or "better" than the network infrastructure in IPv4. However, it is understood that IPv6 is not required to solve current network infrastructure problems not solved by IPv4. It may also not be feasible to deploy IPv6 on all parts of the network immediately.

Scenario 2:   Sparse IPv6 dual-stack deployment in IPv4 network infrastructure. Agency with an existing IPv4 network wishes to deploy a set of particular IPv6 "applications" (application is voluntarily loosely defined here, e.g., peer to peer). The IPv6 deployment is limited to the minimum required to operate this set of applications.

- Assumptions: IPv6 software/hardware components for the application are available, and platforms for the application are IPv6 capable.

- Caveats: Do not disrupt IPv4 infrastructure.

Scenario 3:   IPv6 dominant network infrastructure with some IPv4-capable nodes/applications needing to communicate over the IPv6 infrastructure. An enterprise deploying a new network or restructuring an existing network, decides IPv6 is the basis for most network communication. Some IPv4 capable nodes/applications will need to communicate over that infrastructure.

- Assumptions: Required IPv6 network infrastructure is available, or is available over some defined timeline, supporting the enterprise plan.

---

[1] References to the term "network infrastructure" are defined as the software, network operations and configuration, and methods used to operate a network in an enterprise.

- Caveats: Interoperation and coexistence with IPv4 network infrastructure and applications are required for communications.

Another activity which can assist agencies with requirements gathering is to answer a series of questions about the segments of their network infrastructure. The network infrastructure components are identified below provide an initial template to ascertain the requirements to determine an agency plan to transition to IPv6.

- Network Infrastructure Component 1
  - Agency Provider Requirements
    - Is external connectivity required?
    - One site vs. multiple sites, and are they within different geographies?
    - Is the private wide area network (WAN) infrastructure (e.g., leased lines) shared (e.g., VPNs/ISP)?
    - If the agency has multiple sites, how is the traffic exchanged securely?
    - How many global IPv4 addresses are available to the agency?
    - What is the IPv6 address assignment plan available from the provider?
    - What prefix delegation is required by the agency?
    - Will the agency be multi-homed?
    - What multi-homing techniques are available from the provider?
    - Will clients within the agency be multi-homed?
    - Does the provider offer any IPv6 services?
    - Which site-external IPv6 routing protocols are required?
    - Is there an external data center to the agency, such as servers located at the Provider?
    - Is IPv6 available using the same access links as IPv4, or different ones?

- Network Infrastructure Component 2
  - Agency Application Requirements
    - List of applications in use?
    - Which applications must be moved to support IPv6 first?
    - Can the application be upgraded to IPv6?
    - Will the application have to support both IPv4 and IPv6?
    - Do the enterprise platforms support both IPv4 and IPv6?
    - Do the applications have issues with NAT v4-v4 and NAT v4-v6?
    - Do the applications need globally routable IP addresses?
    - Do the applications care about dependency between IPv4 and IPv6 addresses?
    - Are applications run only on the internal network?

- Network Infrastructure Component 3
  - Agency IT Department Requirements

- Who "owns"/"operates" the network: in house or outsourced?
- Is working remotely (i.e., through VPNs) supported?
- Are inter-site communications required?
- Is network mobility used or required for IPv6?
- What are the requirements of the IPv6 address plan?
- Is there a detailed asset management database, including hosts, IP/MAC addresses, etc.?
- What is the agency's approach to numbering geographically separate sites that have their own Service Providers?
- What will be the internal IPv6 address assignment procedure?
- What sites internal IPv6 routing protocols are required?
- What will be the IPv6 Network Management policy/procedure?
- What will be the IPv6 QOS policy/procedure?
- What will be the IPv6 Security policy/procedure?
- What is the IPv6 training plan to educate the enterprise?
- What network operations software will be impacted by IPv6?
  - DNS
  - Management (SNMP & ad-hoc tools)
  - Enterprise Network Server applications
  - Mail Servers
  - High Availability Software for Nodes
  - Directory Services
  - Are all these software functions upgradeable to IPv6?
  - If not upgradeable, then what are the workarounds?
  - Does any of the software functions store, display, or allow input of IP addresses?
  - Other services (e.g., NTP, etc.)
- What network hardware will be impacted by IPv6?
  - Routers/switches
  - Printers/Faxes
  - Firewalls
  - Intrusion Detection
  - Load balancers
  - VPN Points of Entry/Exit
  - Security Servers and Services
  - Network Interconnect for Platforms
  - Intelligent Network Interface Cards
  - Network Storage Devices
  - Are all these hardware functions upgradeable to IPv6?
  - If not, what are the workarounds?
  - Do any of the hardware functions stores, display, or allow input of IP addresses?
  - Are the nodes moving within the agency network?

- Are the nodes moving outside and inside the agency network?

- Network Infrastructure Component 5
  - Agency Network Interoperation and Coexistence
    - What platforms are required to be IPv6 capable?
    - What network ingress and egress points to the site are required to be IPv6 capable?
    - What transition mechanisms are needed to support IPv6 network operations?
    - What policy/procedures are required to support the transition to IPv6?
    - What policy/procedures are required to support interoperation with legacy nodes and applications?

In addition to the Networking Infrastructure components identified, another exercise that can benefit an agency planning for the transition and deployment of IPv6 is to develop a matrix of the choices it has to deploy IPv6 within its current IPv4 network.

Table 1 shows a matrix of ten possible transitions. The information below was taken from the informational IETF RFC 4057 IPv6 enterprise scenarios document. Agencies may reference this document at ftp://ftp.rfc-editor.org/in-notes/rfc4057.txt.

Implementations may require analysis and the selection of an IPv6 transition mechanism for the notional network. Each possible implementation is represented by the rows of the matrix. The matrix describes a set of notional networks as follows:

- The first column represents the protocol used by the application and below, the IP-capability of the node originating the IP packets. (Application/Host 1 OS)
- The second column represents the IP-capability of the host network wherein the node originated the packet. (Host 1 Network)
- The third column represents the IP-capability of the service provider network. (Service Provider)
- The fourth column represents the IP-capability of the destination network wherein the originating IP packets are received. (Host 2 Network)
- The fifth column represents the protocol used by the application and, below, the IP-capability of the destination node receiving the originating IP packets.(Application/Host 2 OS)

As an example, notional network 1 is an IPv6 application residing on a Dual-IP layer host trying to establish a communications exchange with a destination IPv6 application. To complete the information exchange the packets must first traverse the host's originating IPv4 network (intranet), then the service provider's, and destination hosts Dual-IP network.

Obviously Table 1 does not describe every possible scenario. Trivial notional networks (such as pure IPv4, pure IPv6, and ubiquitous Dual-IP) are not addressed. However, these ten represent the vast majority of transitional situations likely to be encountered in today's enterprise. Therefore, we will use these ten to address an example analysis for enterprise IPv6 deployment.

```
Table 1 - Enterprise Scenario Deployment Matrix


    ========================================================
    |Application |Host 1 |Service |Host 2 |Application |
    |----------- |Network|Provider|Network|----------  |
    | Host 1 OS  |       |        |       | Host 2 OS  |
    =====================================+==============
    |     IPv6   |       |Dual IP |       |     IPv6   |
  A |     ----   | IPv4  |  or    |Dual IP|     ----   |
    |   Dual IP  |       |  IPv4  |       |   Dual IP  |
    ========================================================
    |     IPv6   |       |        |       |     IPv6   |
  B |     ----   | IPv6  | IPv4   | IPv4  |     ----   |
    |   Dual IP  |       |        |       |   Dual IP  |
    ========================================================
    |     IPv4   |       |        |       |     IPv4   |
  C |     ----   | IPv4  |Dual IP | IPv6  |     ----   |
    |   Dual IP  |       |        |       |   Dual IP  |
    ========================================================
    |     IPv4   |Dual IP|        |       |     IPv4   |
  D |     ----   |  or   | IPv4   | IPv6  |     ----   |
    |   Dual IP  | IPv6  |        |       |   Dual IP  |
    ========================================================
    |     IPv6   |Dual IP|        |Dual IP|     IPv4   |
  E |     ----   |  or   |Dual IP |  or   |     ----   |
    |   Dual IP  | IPv6  |        | IPv6  |   Dual IP  |
    ========================================================
    |     IPv6   |       |        |       |     IPv4   |
  F |     ----   | IPv6  | IPv4   | IPv4  |     ----   |
    |   Dual IP  |       |        |       |   Dual IP  |
    ========================================================
    |     IPv4   |       |        |       |     IPv6   |
  G |     ----   | IPv6  | Dual IP| IPv6  |     ----   |
    |   Dual IP  |       |        |       |   Dual IP  |
    ========================================================
    |     IPv4   |       |        |       |     IPv6   |
  H |     ----   | IPv6  |Dual IP | IPv4  |     ----   |
    |     IPv4   |       |        |       |   Dual IP  |
    ========================================================
    |     IPv4   |       |        |       |     IPv6   |
  I |     ----   | IPv6  | IPv4   | IPv6  |     ----   |
    |     IPv4   |       |        |       |   Dual IP  |
    ========================================================
    |     IPv6   |       |        |       |     IPv4   |
  J |     ----   | IPv4  | IPv4   | IPv6  |     ----   |
    |   Dual IP  |       |        |       |   Dual IP  |
    ========================================================
```

The reader should note that scenarios A-C in Table 1 are variations of compatible hosts communicating across largely (but not entirely) homogenous networks. In each of the first three scenarios, the packet must traverse at least one incompatible network component. For example, scenario B represents an enterprise which wishes to use IPv6 applications, but has yet to transition its internal networks - and its Service Provider also lags, offering only a v4 IP-service. Conversely, Scenario C represents an enterprise which has completed transition to IPv6 in its core networks (as has its Service Provider), but continues to require a legacy IPv4-based

Scenario D represents the unusual situation where the enterprise has transitioned its core Intranet to IPv6, but (like scenario B) its ISP provider has yet to transition. In addition, this enterprise continues to retain critical legacy IPv4-based applications which must communicate over this heterogeneous network environment.

Scenarios E-J represents transitional situations where the enterprise has both v4- and v6-based instantiations of the same application that must continue to interoperate. In addition, these scenarios show that the enterprise has not completed transition to IPv6 in all its organic and/or Service Provider networks. Instead it maintains a variety of heterogeneous network segments between the communicating applications. Scenarios E and J represent distinctly different extremes on either end of the spectrum. In scenario E, the enterprise has largely transitioned to IPv6 in both its applications and networks. However, scenario E shows that a few legacy IPv4-based applications may still be found in the enterprise. On the other hand, scenario J shows an enterprise that has begun its transition in a very disjointed manner and, in which IPv6-based applications and network segments are relatively rare.

Agencies serving as Network Providers can also review the IETF RFC 4029 Scenarios and Analysis for Introducing IPv6 into ISP Networks at ftp://ftp.rfc-editor.org/in-notes/rfc4029.txt.   Additionally, since Seamless Mobility is considered to be one of IPv6 advantages over IPv4, an analysis for these networks can be reviewed within IETF RFC 4215 Third Generation Partnership Project (3GPP) Networks at ftp://ftp.rfc-editor.org/in-notes/rfc4215.txt.

Appendix C: Transition Mechanisms

Listed below is a description of the different transition mechanisms options available to an agency to ensure IPv4 and IPv6 interoperability. These mechanisms are categorized in the following three broad classes: dual-stack, tunnels (includes configured and automatic tunnels), and translation mechanisms.

Dual-stacks

The term "dual-stack" refers to TCP/IP capable devices providing support for both IPv4 and IPv6. It is important to understand that having a device being able to communicate over both IPv4 or IPv6 does not necessarily means that all applications operating within this device are capable of utilizing both IPv4 and IPv6. The term "Dual-stack routing" refers to a network that is dual IP, that is to say all routers must be able to route both IPv4 and IPv6.

Requiring all new devices be both IPv4 and IPv6 capable permits these devices to have the ability to use either IP protocol version, depending on the services available, the network availability, service, and the administrative policy. A transition scenario which calls for "dual-stack everywhere" provides the most flexible operational environment. Dual-stacked hosts running on a dual-stack network allow applications to migrate one at a time from IPv4 transport to IPv6 transport. Legacy applications and devices that are not yet upgraded to support access to the IPv6 stack can coexist with upgraded IPv6 applications on the same network system.

Tunnels

The term "tunneling" refers to a means to encapsulate one version of IP in another so the packets can be sent over a backbone that does not support the encapsulated IP version. For example, when two isolated IPv6 networks need to communicate over an IPv4 network, dual-stack routers at the network edges can be used to set up a tunnel which encapsulates the IPv6 packets within IPv4, allowing the IPv6 systems to communicate without having to upgrade the IPv4 network infrastructure that exists between the networks.

Configured Tunnels

The term "configured tunnels" is used when network administrators manually configure the tunnel within the endpoint routers at each end of the tunnel. Any changes to the network like renumbering must be must manually reflected on the tunnel endpoint. Tunnels result in additional IP header overhead since they encapsulate IPv6 packets within IPv4 (or vice versa).

Automatic Tunnels

The term "automatic tunnels" is used when a device directly create their own tunnels to dual-stacked routers for shipping IP packets within IP. The IPv6 Tunnel Broker (RFC 3053), 6to4 (RFC 3056), Teredo (Tunneling IPv6 over UDP through NATs) and ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) ship IPv6 packets within IPv4 and can be referenced as IPv6-over-IPv4 mechanisms while DSTM (Dual-stack Transition Mechanism) ships IPv4 packets within IPv6 and can be reference as IPv4-over-IPv6 mechanism.

The IPv6 tunnel broker mechanism uses dual-stacked servers sitting between IPv6 and IPv4 networks to assist in the set up of a configured tunnel to a host. 6to4, Teredo and ISATAP allow end host systems to create their own automatic tunnels to dual-stacked routers for shipping IPv6 packets within IPv4. While ISATAP is mainly for IPv6-over-IPv4 tunneling within a domain, all of the other IPv6-over-IPv4 mechanisms are designed to tunnel IPv6 packets out of an IPv4-only administrative domain. Like configured tunnels, automatic tunneling has double IP header overhead, since tunnels encapsulate IPv6 packets within IPv4 (or vice versa).

DSTM technique provides a unique solution to the IPv4-IPv6 transition problem. This mechanism is designed to rapidly reduce the reliance on IPv4 routing and is intended for IPv6-only networks in which hosts still occasionally need to exchange information directly with other IPv4 hosts or applications. Network administration is simplified and the need of IPv4 global addresses is reduced. DSTM can be integrated with an IPv6 Tunnel Broker for tighter security integration. DSTM routers can be coupled with IPv4 Firewalls and Intrusion Detection systems to secure IPv4 tunnel endpoints from IPv4-based attacks.

Special consideration must be given to the security risk associated with automatic tunneling as it allows user-nodes to establish tunnels that may bypass a site's security checkpoints such as firewalls and intrusion detection systems. In general, a full dual-stack along with IPv6-capable firewalls, guards, intrusion detection, and end-host security may provide a more secure and interoperable IPv6 transition solution than tunneling. However, for network infrastructures that contain IPv4-only or IPv6-only routing coupled with dual-stack end-nodes, automatic tunneling provides a flexible transition strategy. Again the risks associated with all potential solutions must be carefully considered.

Protocols Translators

The term "translators" refers to devices capable of translating traffic from IPv4 to IPv6 or vice and versa. This mechanism is intended to eliminate the need for dual-stack network operation by translating traffic from IPv4-only devices to operate within an IPv6 infrastructure. This option is recommended only as a last resort because translation interferes with objective of end-to-end transparency in network communications. Use of protocol translators cause problems with NAT and highly constrain the use of IP-addressing.