



**Federal Government Transition
Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6)**

Frequently Asked Questions - Update

1/7/07

BACKGROUND

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

Internet Protocol is the “language” and set of rules computers use to transmit data 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 location on the Internet. IPv6 provides the world with an almost unlimited number of available IP addresses, as well as significantly enhanced mobility features. Therefore, IPv6 is paramount to the continued growth of the Internet and development of new applications leveraging mobile, Internet connectivity. Although the IT community has come up with workarounds for this shortage in the IPv4 environment, IPv6 is viewed as the true long-term solution to this problem.

OMB Memorandum M-05-22 identifies several key milestones and requirements for all Federal Executive Branch agencies in support of the June 30, 2008 IPv6 transition date. 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

The directive is available at <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf>.

GENERAL QUESTIONS

Why has the Federal government mandated transition to IPv6?



The Federal government has requested all agencies transition their network backbones to IPv6 for the following reasons:

- To take advantage of the expanded IP address space, and embrace future-oriented networking capabilities, such as converged communications, IP-aware medical devices, remote sensors, etc.
- To address the challenge faced by the U.S. from international competition in the realm of IPv6
- To lead by example in U.S. enterprise IPv6 transformation

What does “network backbone” mean? What is the scope of the mandate?

For the purposes of the Federal government IPv6 transition, the “network backbone” is the network core. The core is the set of network transport devices (e.g. routers, switches) providing the highest level of traffic aggregation in the network, and thus forming the highest level of hierarchy in the network. This includes network transport devices that provide access to the Internet (e.g., Internet edge routers). From a traffic flow perspective, the core supports transient traffic only – i.e., there are no traffic sources or destinations on the core network.

Are desktops, network peripherals, or applications included in the mandate?

No. The requirements for June 30, 2008 are for the network core only. 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.

What do agencies need to accomplish by 2008 to be considered compliant with OMB Memorandum M-05-22?

OMB Memorandum M-05-22 requires the agency’s network core to be capable of supporting both IPv4 and IPv6 (addresses and traffic) by June 30, 2008. Agencies need to be able to demonstrate they are capable of performing at least the following success criteria, without compromising IPv4 capability and network security:

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

For these demonstrations, the term “LAN” represents IPv6-configured PCs/laptops (with associated cabling and switching as needed), directly connected to IPv6 devices (e.g. routers, switches) in an agency’s operational core backbone network. The term “Internet and external peers” refers to an external network (i.e. a network owned and operated by an organization different from that agency) chosen for the demonstrations, and which may be from a partner agency, ISP, or other IPv6 organization. The external network contains equipment outside of the agency’s own control or purview.



Connectivity between the agency's demonstration network and the external peer(s) may be established from either a dedicated circuit, such as a leased line, or via the public Internet.

It is emphasized that the demonstrations of compliance with the M-05-22 memorandum must be performed on the agency's operational core network.

These requirements are described in further technical detail in the CIO Council document, "Demonstration Plan to Support Agency IPv6 Compliance." The Demonstration Plan includes a description of the evidence agencies should generate to document successful completion of these tests. This document is currently undergoing review and approval processes, and will be available at www.cio.gov (See section: Documents; IPv6).

What should agencies send to OMB on (or before) June 30, 2008 to demonstration compliance with M-05-22?

OMB will soon be releasing a memorandum to agencies which details these requirements. In anticipation of this memo, agencies should compile documentation as recommended by the CIO Council document, "Demonstration Plan to Support Agency IPv6 Compliance."

How can an agency determine if an IT product is compliant with the requirements of M-05-22?

In support of the June 2008 deadline, agencies are to determine what their specific requirements are and develop procurement language accordingly. To assist agencies in determining both their near-term and longer-term requirements, the National Institute of Standards and Technology (NIST) released a draft IPv6 standards profile for the Federal government ("NIST Special Publication 500-267, A Profile for IPv6 in the U.S. Government - Version 1.0"). This draft profile was released in January 2007, and was open for public comment through March 2007. Version 1.0 has been updated based on this feedback, and will be released again for a final, 30-day public comment period in January 2008. After this 30-day public comment period, Version 1.0 of the profile will be updated accordingly, and released by NIST in its final format. NIST will make revisions to the standards profile should additional requirements evolve in the future.

This publication supports longer-term planning activities (beyond June 2008) and provides a standards profile to assist Federal agencies in developing plans to acquire and deploy products that implement IPv6. The profile recommends IPv6 capabilities for common network devices, including hosts, routers, intrusion detection systems, and firewalls, and includes a selection of IPv6 standards and specifications needed to meet the minimum operational requirements of most Federal agencies.

At the recommendation of NIST, the Federal government will be facilitating the establishment of a lab accreditation and product testing program which will allow *any accredited public and private testing laboratory* to test and certify products for conformance with the Federal government IPv6 standards profile. This will allow product vendors to use any accredited test lab to "self-certify" its products meet the requirements of the standards profile (and hence, the requirements of M-05-22). Upon successful testing, vendors will maintain a Supplier's Declaration of Conformity (ISO/IEC 17050-1:2004). Agencies will interpret this Declaration of Conformity as compliance with the Federal government IPv6 standards profile.



The Federal government will control the technical content of the NIST standards profile and the attributes of the testing program. NIST will not conduct any product conformance testing. Rather, NIST will identify the lab accreditors and establish the testing requirements (e.g. test suites). The actual product testing will be done by the public and private test labs accredited by a lab accreditation body. Under this plan, any public or private test lab can become accredited to test IPv6 products against the Federal government IPv6 standards profile. This includes test labs already operating within the Federal government.

What is the difference between lab accreditors and test labs?

The test labs are the entities that will be performing the validation of products against the standards profile.

The lab accreditors are the bodies certifying which test labs are capable of performing this validation. This involves the assessment of the systems and methods used by a lab to ensure the lab is competent to perform specific tests or calibrations.

How can I learn more about plans for the testing program?

NIST will host a lab accreditors meeting on February 19, 2008. Any lab accreditation body with interest in participating should attend this meeting. This meeting is primarily oriented towards lab accreditors. However, there will be a general discussion of the testing program. The meeting will be announced in the Federal Register shortly after the release of the standards profile in January 2008. The Federal Register is the official daily publication for rules, proposed rules, and notices of Federal agencies and organizations, as well as executive orders and other presidential documents. Its contents can be accessed at www.regulations.gov.

Since the meeting on February 19, 2008 is oriented towards lab accreditors only, the General Services Administration (GSA) will be hosting an IPv6 Industry Day in the March 2008 timeframe. This meeting will be a forum where test labs, product vendors, and other interested parties can learn more about this plan. The date and details of this meeting will also be announced by GSA in the Federal Register in the coming weeks.

Will the establishment of a Federal government IPv6 standards profile divide the IPv6 marketplace? Hasn't an industry-wide profile already been developed (e.g. IPv6 Ready Logo)?

The Federal government IPv6 standards profile is biggest step towards global integration of IPv6 standards that industry will have seen to date. NIST has been actively engaged with members the IPv6 community world-wide throughout the development of the profile, including the IPv6 Forum (world-wide consortium), the TAHI group (Japan), and the IPv6 Ready Logo program at the University of New Hampshire Interoperability Testing Lab (UNH-IOL).

When can vendors begin testing their products against the profile?

It is estimated it will take NIST 12 to 24 months (from January 2008) to fully establish the lab accreditation program and test suites. Therefore, agencies should expect at least this amount of time before vendors are able to test their products against the Federal government IPv6 standards profile in accredited test labs. During this timeframe, agencies should develop procurement language that aligns with this longer-term goal. Vendors should continue to develop products in



alignment with the Federal government IPv6 standards profile, in anticipation of the accredited test labs.

Will there be an IPv6 Federal Acquisition Regulation (FAR) clause?

The FAR Council is in the process of reviewing the Federal government plans related to lab accreditation, test labs, and Supplier Declaration of Conformity, and will be making its final recommendation in the coming months. Agencies and vendors are encouraged to align their efforts with the requirements of the Federal government IPv6 standards profile, and the plans noted above.

Are agencies expected to acquire their own IPv6 address space?

Yes. Unless an agency is exclusively using a commercial Internet Service Provider (ISP) for network services (in which case, the ISP will “loan” the agency the addresses), agencies are expected to obtain their IPv6 address blocks directly from the American Registry for Internet Numbers (ARIN) www.arin.net .

It is understood it is difficult for agencies to precisely gauge their future IP address needs. However, agencies should be aware IPv6 address requirements will likely be significantly greater than agency IPv4 address requirements resulting from the removal of Network Address Translation (NAT) and the emergence of more IP-aware devices and applications in the future.

What is expected of agencies after June 30, 2008?

The adoption of IPv6 provides Federal government agencies with new technological capabilities, such as mobile IP, improved multicast and Quality of Service (QoS), and the ability to dedicate unique IP addresses to a nearly unlimited number of hosts. Agencies are expected to begin leveraging these new capabilities to better serve the information needs of the public and the Federal government. Agencies’ strategic planning activities should be done with these new capabilities in mind. The Government and the private sector have already begun to develop business cases for the use of IPv6.

How does the Federal government Trusted Internet Connections (TIC) effort (OMB Memorandum M-08-05) affect agencies’ ability to meet the June 30, 2008 deadline for IPv6?

The June 2008 deadline for IPv6 adoption is consistent with the implementation date for the Trusted Internet Connections (TIC) initiative. The TIC initiative is expected to greatly improve security through the reduction of civilian government external connections, including their Internet connections. Agencies should integrate their current and future IPv6 planning with their planning for the TIC effort.

The OMB Trusted Internet Connections memorandum is available at:
<http://www.whitehouse.gov/omb/memoranda/fy2008/m08-05.pdf> .

Where can Federal government personnel working on the IPv6 effort go to share information?

The Architecture & Infrastructure Committee (AIC) of the CIO Council started a Federal IPv6 Working Group in February 2006. Agency IPv6 leads were contacted about the Working Group,



and the first meeting was hosted on February 15, 2006. The group has continued to meet monthly since that time. The Working Group membership is limited to Federal government personnel only. The Working Group is co-chaired by Peter Tseronis (Department of Education; Peter.Tseronis@ed.gov).

Is guidance available to Federal government agencies?

The CIO Council Architecture and Infrastructure Committee (AIC) has published IPv6 implementation guidance, which is available on the CIO Council website at: <http://www.cio.gov/index.cfm?function=showdocs&category=7> .

The first chapter of this guidance addresses the use of Enterprise Architecture (EA) to plan for enterprise-wide IPv6 transition. This chapter also includes instructions to agencies on how to submit their IPv6-related artifacts with their February 28, 2006 Enterprise Architecture assessment. The second chapter discusses 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 discusses IPv6 transition governance. It describes the management structure of the Government-wide IPv6 transition effort, the roles and responsibilities of each of the agencies and organizations involved (e.g. OMB, CIO Council, large and small agencies), and key points of contact for the Federal government IPv6 effort.

The Federal IPv6 Working Group also regularly distributes guidance materials to its members, and facilitates IPv6 implementation discussions at its monthly meetings.

How can those outside of the Federal government (e.g. private industry, academia, state/local government) contribute to the IPv6 effort?

Open dialogue and information sharing between the Federal government and those in private industry, academia, etc. is encouraged and necessary in order to facilitate the successful adoption of IPv6. Individuals and organizations outside of the Federal government are encouraged to contact the IPv6 Working Group (above) to determine how their input can be appropriately leveraged.