E·GOV

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

Frequently Asked Questions

2/15/06

BACKGROUND

In August of 2005, the Office of Management Budget issued Memorandum 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 05-22 identifies several key milestones and requirements for all Federal government 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 do agencies need to accomplish by 2008 to be considered compliant with OMB Memorandum 05-22? Does just the network backbone need to be transitioned, or are applications and peripherals also included?
OMB Memorandum 05-22 requires the agency's network backbone (aka. "network core") to be capable of transmitting both IPv4 and IPv6 traffic, and supporting IPv4 and IPv6 addresses, by June 30, 2008. Agencies must be able to demonstrate they are capable of performing at least the following functions, without compromising IPv4 capability or network security:

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

The requirements for June 30, 2008 are for the network backbone (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.

Agencies should verify this new capability through testing activities. Agencies are required to maintain security during and after adoption of IPv6 technology into the network core**.**

Will OMB or the CIO Council be publishing guidance to agencies on IPv6 transition?
The CIO Council Architecture and Infrastructure Committee (AIC) will be publishing IPv6 implementation guidance in a "chapter" format. There will be a series of four chapters.

The first chapter, published on November 15, 2005, 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, 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 fourth chapter discusses acquisition and procurement of IPv6-capable assets. It describes the Federal Acquisition Regulation (FAR) clause being implemented in support of IPv6 transition.

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. After the comments are reviewed and incorporated, the documents will be posted on the CIO Council and OMB E-Gov web sites (*www.cio.gov; www.e-gov.gov*).

The fourth chapter of transition guidance is currently under review. Once it is complete, it will be sent directly to agency IPv6 leads for comment, and subsequently posted to the CIO Council and OMB E-Gov web sites.

Are agencies required to procure only IPv6-capable assets (hardware/software)?
Yes, to the maximum extent practicable. OMB memorandum dated August 2, 2005 requires all agencies' network backbones to be capable of transmitting IPv6 traffic by June 30, 2008. Agency infrastructure must be able to successfully interface with this updated network backbone. Additionally, the memorandum states, "To avoid unnecessary costs in the future, you should, ensure that all new IT procurements are IPv6 compliant. Any exceptions to the use of IPv6 require the agency's CIO to give advance, written approval." As necessary, agencies should develop internal policies to address this requirement.

What is the definition of "IPv6-capable" for the Federal government?
When discussing Federal government transition to IPv6, there are two uses of the term "IPv6-capable." The first refers to the high level requirement to make agency network backbones "IPv6-capable." This means that the network backbone is capable of successfully passing IPv6 data traffic, and supporting IPv6 addresses. This term does not imply the backbone is actually doing so, but rather it is *capable* of doing so. The term "IPv6-enabled" is the term used to more accurately describe a network backbone that is not only capable of supporting IPv6, but is actually "turned on" – implying IPv6 traffic is actually successfully passing through the network. The terms "IPv6 compliant" and "using IPv6" used in OMB Memorandum 05-22 are synonymous with "IPv6-capable."

The second use of "IPv6-capable" refers to the technical specifications of an IT product or device, such as a router, switch, firewall, or computer operating system. This is critical to ensure interoperability between products and networks. At the current time, there is not a unified Federal government technical specification for "IPv6-capable."

OMB Memorandum 05-22 states: "Specifically, any new IP product or system developed, acquired, or produced must, if not initially compliant, provide a migration path and

commitment to upgrade to IPv6 for all application and product features by June 2008." What does this mean?
If an agency must acquire an IT asset that is not IPv6-capable (i.e., IPv6-capable version is not yet available), yet is integral to the transition of the network backbone, the agency must ensure this asset is upgraded by June 30, 2008.

What does "backbone" mean?
The "backbone" includes the wide area network (WAN) core up to the local area network (LAN) point of demarcation. The LAN demarcation point is the device (e.g., router, switch) which services the workstations.

If agencies are not receiving additional funding for this transition, how will agencies pay for this?
For the most part, your typical technology refresh will be adequate for the upgrade and/or replacement of all affected IP-aware devices or products.

An agency's normal tech refresh cycle for some IT assets might extend beyond 2008. Will exceptions to the 2008 deadline be made for these assets?
No. Assets which have a lifetime beyond 2008 are assumed to be relatively recent and upgradeable.

Are agencies expected to acquire their own IPv6 address space?
The address acquisition process is a rigorous one. Therefore, the government will be best served by having a central point of coordination for these efforts.

To help facilitate the address space acquisition process, the Government intends to have a central point of coordination, the National Telecommunications and Information Administration (NTIA), for these efforts. The NTIA, within the Department of Commerce, will facilitate and assist agencies as they interface with ARIN.

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.

More information on the address acquisition process will be announced to agencies shortly, and will also be included in Chapter 3 (Governance) of the CIO Council IPv6 guidance.

Will there be an IPv6 working group for agency IPv6 leads?
Yes. The IPv6 working group is being sponsored and led by the Architecture & Infrastructure Committee (AIC) of the CIO Council. Agency IPv6 leads were contacted about the working group plans and the first meeting was hosted on February 15, 2006.

OMB Memorandum 05-22 instructs agencies to submit their agency IPv6 transition plan with their February 28, 2006 Enterprise Architecture assessment. However, Chapter 1 of

the CIO Council guidance instructs agencies to submit their Enterprise Architecture Transition Strategy instead of the transition plan. What should agencies submit?
Agencies should submit their Enterprise Architecture Transition Strategy with the February assessment. OMB Memorandum 05-22 does say agencies are required to create an IPv6 transition plan. However, OMB is not going to require they submit a separate IPv6 transition plan with their EA assessment. Agencies may do so, but it is not required.

OMB is more concerned the agency's IPv6 transition milestones and project/program interdependencies are reflected in the EA Transition Strategy. So, essentially, the agency's internal IPv6 transition plan should be integrated within the agency's EA Transition Strategy.

Non-scorecard agencies do not undergo Enterprise Architecture assessments, and do not have Enterprise Architecture Transition Strategies. How should these agencies meet the February, 28, 2006 requirements?
As mentioned above, agencies without an EA Transition Strategy should submit their IPv6 Transition Plan, along with their IPv6 progress report, to *ipv6@omb.eop.gov*.

DEVICE INVENTORY QUESTIONS

When are the inventories due?
The first inventory was due to OMB on November 15, 2005. The second inventory is due to OMB on June 30, 2006.

What should agencies include in the first inventory?
Inventory data on existing routers, switches, and hardware firewalls for your agency's WAN up to the LAN point of demarcation.

What should agencies include in the second inventory?
The second inventory should consist of any IP-aware devices and technologies which are components of your network backbone transition, but not captured in the first inventory.

The first inventory focused on network backbone hardware devices only. The second inventory should reflect any other technologies or devices (not included in the first inventory) which need to be upgraded/replaced/modified in order to achieve a successful backbone transition. For example, if there are any other IT assets which need to be upgraded in order to make the network backbone capable of supporting IPv6 (e.g. DHCP server and/or software), they should be included in this second inventory.

Should agencies include vendor-owned IP devices and technologies in their inventories?
If the contract term for the vendor-owned IP devices expires before June 2008, then agencies do NOT need to include the devices in the inventory because the agency will re-compete the contract and require all new contractor-provided IP devices be IPv6-capable. However, if the contract term for the vendor-owned IP devices expires after June 2008, then agencies DO need to include the devices in your inventory because agencies will not be able to re-compete the

contract to ensure the contractor provides IPv6-capable devices.

How should agencies submit their inventory data?
Agencies should submit their inventories by sending it to *ipv6@omb.eop.gov*, or by burning the inventory to a CD-ROM and hand carrying it to the New Executive Office Building, 725 17th Street, N.W., Washington, D.C., 20503 . If you choose to submit the inventories in person, you will need to call ahead and make sure someone is available at the New Executive Office Building to receive it. Please contact Carol Bales at *Carol_Bales@omb.eop.gov*; 202-395-9915.

Will these inventories be classified?
If the inventory contains classified information, it may be classified and submitted as such. If you wish to make a classified submission, please contact Carol Bales at *Carol_Bales@omb.eop.gov*; 202-395-9915.

In section 2, "Investment Information" what constitutes a site (building, data center, campus, city, etc)?
Depending upon the type of investment, a site may be any one of the listed examples, e.g., a building, data center, campus, city, military base, regional network.

In section 3, is OMB looking for a summary of devices? What if we have 30 of the same device?
For the first inventory submission (due November 11, 2005), an inventory of each device is required rather than a summary of the devices. This is true for both portions of section 3 (the question and the "details worksheet"). For section 4, you may summarize by model of device.

For the second inventory submission (due June 30, 2006), agencies may summarize by model in both sections 3 and 4. If summarized data is submitted, a count of devices must also be included. Agencies may modify the worksheet as needed to include this extra information.

In section 3, should the Application and Device Inventory include details from both #3 and #4?
Yes. Section 3 should include all application and devices in the investment (compliant and non-compliant), and Section 4 should break out just the non-compliant devices, i.e., those requiring upgrade or replacement. In other words, the applications/devices listed in a Section 4 should be a subset of those listed in Section 3.

If devices are largely under a seat contract, should only seat charges be reported?
Agencies can report monthly seat charges, but should make a note that this is what is being reported.

In the "Supported Standards" section, is this relative to IPv6 or all standards?
This is only those standards relative to IPv6.

In the "Device Security/Criticality" section, what standard should be used to determine this?
Agencies should use FIPS 199: Low, Moderate, or High.

Firewall monitoring of tunneled IPv6 traffic (Type 41 packets) and Deep Packet Inspection: How do we answer this if the answer is not "yes" or "no" for both?
Agencies should answer "yes/no" or "no/yes" depending upon which of the answers is valid, i.e., if the Firewall performs monitoring of tunneled IPv6 traffic (Type 41 packets) but does NOT perform Deep Packet Inspection, then the correct response would be "yes/no."

What should be included in the "known issue" column?
This column should show if there are any known interoperability or security issues with the device once it has been made IPv6 capable.