Federal Government Adoption
of Internet Protocol Version 6 (IPv6)

Frequently Asked Questions

Updated: November 4, 2011

BACKGROUND

In September 2010, OMB issued a memorandum requiring federal agencies to operationally deploy native Internet Protocol Version 6 (IPv6) for public Internet servers and internal applications that communicate with public servers. This new directive builds upon an August 2005 memorandum, M-05-22, which established the goal of deploying IPv6 in all Federal government agency network backbones by June 30, 2008. OMB also issued an IPv6 Roadmap in May 2009 that built upon requirements set forth in the August 2005 memorandum.

The Internet Protocol (IP) is the "envelope" and set of rules computers use to deliver 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 address on the Internet. IPv6 provides the world with a virtually unlimited number of available IP addresses[1], significantly enhanced mobility features, and the opportunity to increase the ubiquity of network security capabilities. Therefore, adoption of IPv6 is viewed as being vital to the long-term continued growth of the Internet and development of new applications that leverage robust end-to-end Internet connectivity.

GENERAL QUESTIONS

Why has the Federal government mandated adoption of IPv6?

The rapid exhaustion of the global IPv4 address space will have a negative impact on the growth of Internet use, the innovation of new services, the robustness of existing services, and the cost and complexity of network operations based upon IPv4. While many near term engineering fixes are being developed to prolong the inevitable, over the long-term the wide-scale adoption and deployment of IPv6 is necessary to maintain the business-continuity of the Internet.

The Federal government has requested all agencies adopt IPv6 in order to:

- Enable the successful deployment and expansion of key Federal information technology (IT) modernization initiatives, such as Cloud Computing, Broadband, and SmartGrid, which rely on robust, scalable Internet networks;
- Reduce complexity and increase transparency of Internet services by eliminating the architectural need to rely on Network Address Translation (NAT) technologies;

[1] IPv4 provides a 32 bit address, or approx. 4.2×10^9 addresses.
IPv6 provides a 128 bit address, or approx. 3.4×10^{38} addresses.

- Enable ubiquitous security services for end-to-end network communications that will serve as the foundation for securing future Federal IT systems; and,
- Enable the Internet to continue to operate efficiently through an integrated, well-architected networking platform and accommodate the future expansion of Internet-based services.
- Maintain continuity of operations, and to reach and be reached by customers.

What is required by the September 2010 OMB directive, and to whom does the directive apply?

In accordance with the September 2010 memorandum issued by OMB, agencies are to:

- Upgrade public external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012[2];
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014;
- Designate an IPv6 Transition Manager to serve as the person responsible for leading the agency's IPv6 transition activities, and liaise with the wider Federal IPv6 effort as necessary; and,
- Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program to control the completeness and quality of IPv6 capabilities during acquisition.

The directive applies to unclassified information systems within the Federal Executive Branch Departments and Agencies and builds upon the Federal government's previous work in the area of IPv6. A copy of the September 2010 memorandum can be located at http://www.cio.gov/Documents/Transition-to-IPv6.pdf.

How can progress toward these goals be tracked across all Federal networks?

OMB, in coordination with the IPv6 Task Force, will define the official processes for agencies to report progress with respect to these policies. There are several test and measurement tools that might be useful in characterizing overall progress and the status of individual agencies and networks. Such tools include:

- NIST's IPv6 Deployment Monitor is a measurement tool that attempts to estimate the status of IPv6 enabled external facing services across the federal government. Currently the monitor tests the status of WWW, Email and DNS services and tracks the progress of IPv6 deployment over time. The IPv6 Deployment monitor can be accessed at:
  - http://fedv6-deployment.antd.nist.gov/
- Other tools exist to test the IPv6 capabilities of local access and transit networks. These tools might be of use to agencies in testing IPv6 ISP services. Some examples include:
  - http://test-ipv6.com/
  - http://netalyzr.icsi.berkeley.edu/

[2]To ensure interoperability, it is expected that agencies will also continue running IPv4 into the foreseeable future.

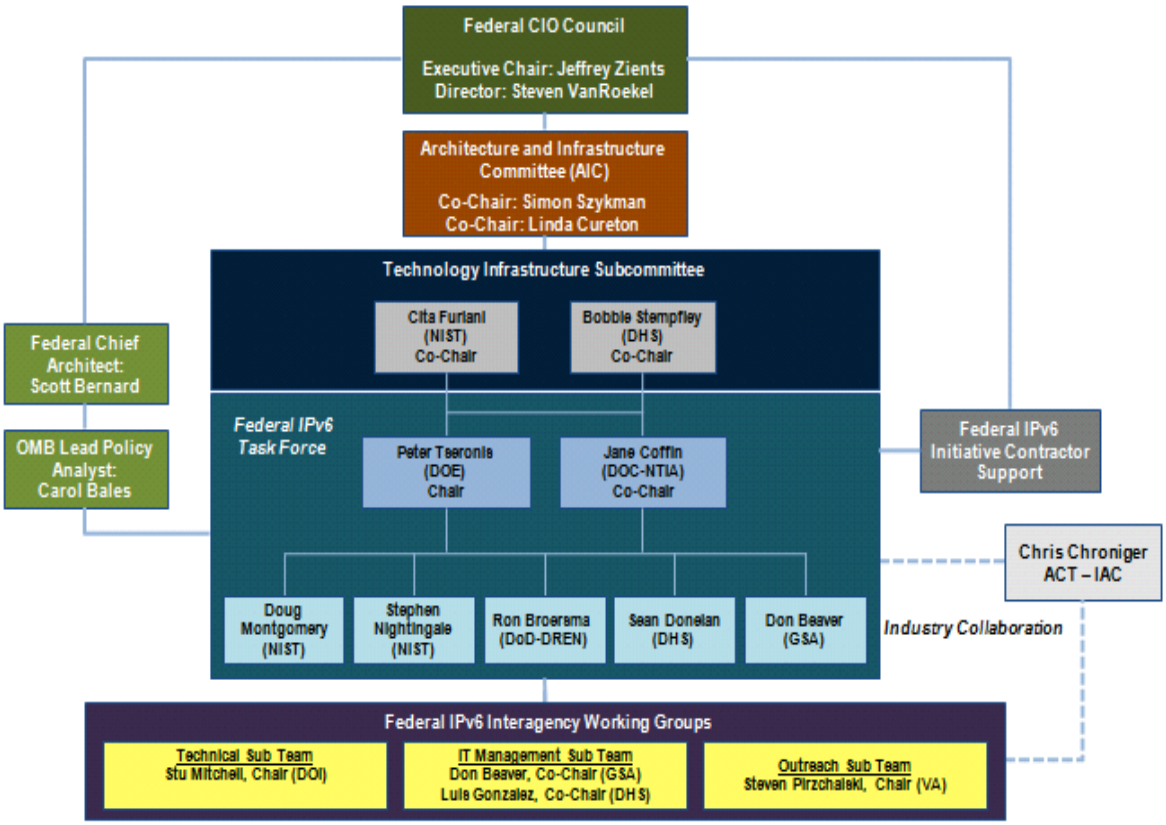
There are numerous other tools, testing efforts and surveys that attempt to characterize the state of IPv6 deployment in the Internet. As other useful tools are identified, they will be shared and discussed with Agency Transition Managers through Task Force meetings and mailing lists.

What is the role of the Federal IPv6 Task Force?

The Federal IPv6 Task Force was established by the Federal CIO Council as part of the Architecture and Infrastructure Committee (AIC). The role of the Task Force is to assist and coordinate agency activities in response to OMB's IPv6 policies. The Task Force's extensive technical and policy experience with IPv6 enables continuity of knowledge to help integrate USG IPv6 activities with the worldwide Internet community.

The diagram below shows the primary points of integration for the Task Force, within the Federal IT Management community:

To contact the Task Force please email: v6task-force@nist.gov



What is expected of Agency IPv6 Transition Managers?

Agency Transition Managers represent their agencies IPv6 efforts to OMB and other federal agencies. Moreover, the Transition Manager should be capable of communicating across the technical and executive perspectives necessary to manage a successful adoption.

Transition Managers should educate themselves on the importance of IPv6 to America's Innovation Agenda and the global Internet community. In addition, Transition Managers are expected to build the necessary structures within their respective organizations to champion and manage a successful adoption of IPv6 enabled services. Finally, Transition Managers are encouraged to communicate the impact of IPv6 efforts within agency architectures to the Federal IPv6 Task Force and OMB.

The group of agency appointed Transition Managers can be contacted through the email list fedv6-deploy@nist.gov.

What guidance available to Federal agencies?

The CIO Council Architecture and Infrastructure Committee (AIC) has published a "*Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government*" (Roadmap) which is available at http://www.cio.gov.

The Roadmap was created through collaboration between public and private partnerships and is intended to aid Federal IPv6 deployment and management efforts. The Roadmap outlines a vision for network modernization and provides specific guidance for agencies on how to integrate this effort within each agency's IT management environment.

The *"Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government"* should be the basis of an agency's IPv6 efforts and help provide a strong foundation to energize and guide agencies to transition to and ultimately adopt IPv6.

The Federal IPv6 Task Force will also regularly distribute guidance materials to the IPv6 Interagency Working Group members, and facilitate IPv6 implementation discussions at its monthly meetings.

Will additional guidance be provided to agencies as they develop/refine their IPv6 transition plans?

This list of Frequently Asked Questions provides additional guidance and interpretation of current OMB policies on this issue, and any additional guidance will be communicated via the IPv6 Interagency Working Group meetings.

Since 2005, agencies have been continually briefed on IPv6 and the importance of adoption. As a result, most agencies have planned for IPv6 in their IT modernization and technology refresh activities. Additionally, the December 2009 modification to the FAR (see below) requires that

agencies address the use of the USGv6 tools (Standards Profile and Testing Program) in their acquisition planning activities. It is important the IPv6 initiative be articulated within agency Enterprise Architecture, CPIC and IT Governance processes.

Agency IPv6 Transition managers should identify opportunities for further information sharing. Furthermore, the IPv6 Task Force, CIO Council and the ACT/IAC organization will help communicate industry best practices and share USG implementation experiences

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

In addition to attending the IPv6 Interagency Working Group meetings and other government sponsored sessions, agency staff can share information via the IPv6 wiki page at https://max.omb.gov/community/x/EhPVI.

For access to the collaborative area on the MAX Federal Community for the Federal IPv6 Interagency Working Group, Federal employees or contractors of Federal agencies must have a MAX user-id, which can be requested at the main MAX Portal: https://max.omb.gov/maxportal/

The IPv6 wiki page is visible on the E-Gov Community home page, where it's listed by its title: "Federal Pv6 Interagency Working Group."

In addition to the wiki, an email distribution list has been established for all Transition Managers: fedv6-deploy@nist.gov. Transition Managers should feel free to use that list to discuss issues that may be of interest to other Transition Managers and support staff.

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. Clearly, the Federal IPv6 deployment initiative will require the direct involvement and close collaboration with Internet equipment and service vendors. Individuals and organizations outside of the Federal government are encouraged to contact the IPv6 Task Force to determine how their input can be appropriately leveraged.

A formal industry IPv6 working group has been established by the American Council for Technology, Industry Advisory Council (ACT-IAC). For more information please contact Chris Chroniger: cchroniger@gmail.com.

How does the Federal government Trusted Internet Connections (TIC) effort (OMB Memorandum M-08-05) affect agencies' ability to meet the new deadlines for IPv6?

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 Federal IPv6 Task Force will work closely with a number of IT governance activities across the government, including the Cloud Computing Program Management Office, Networx Program, and the TIC initiative to ensure congruence. Each of these efforts seeks to assist agencies in their IT infrastructure modernization efforts, and representatives are encouraged to assist in ensuring compatibility.

The OMB Trusted Internet Connections memorandum is available at:
http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf

SCOPE AND APPLICABILITY QUESTIONS

What is the rationale for this specific set of deployment, acquisition and management requirements?

While the Internet industry was slow to adopt IPv6 in the first years after its standardization, the current IPv4 addressing exhaust is motivating a rapid increase in the planning, deployment and use of IPv6 technologies. In the last year we have seen the exhaustion of the IANA free pool of IPv4 addresses and the first significant announcements/deployment of IPv6-enabled access networks and Internet services. Some of these deployments will be IPv6-only, meaning that interoperability with clients/servers that are not IPv6-enabled will require use of transition technologies that typically have negative impacts on the complexity, resilience and cost of network operations.

In order to ensure that Federal agencies remain out in front of the IPv6 adoption and are not blind-sided by the sudden realization of latent industry plans, the September 2010 OMB directive defines a set of deployment, acquisition and management requirements aimed to ensure the timely adoption of IPv6 in the Federal Government. While previous directives (e.g., OMB-05-22) required agencies to plan for the general adoption of IPv6, the 2010 directive defines new requirements meant to bring these plans into implementation with specific milestones.

What is the broader intent of these requirements?

The broad intent of these requirements is to set in motion the general broad adoption of IPv6 in Federal information systems. From this point forward, IPv6 technologies should be addressed in all system design, acquisition, and deployment plans. The requirement to designate IPv6 Transition Managers to lead and report on agency's plans and process and the establishment of the Federal IPv6 Task Force is meant to provide the sustaining coordination necessary to efficiently achieve the ultimate goal.

How do the acquisition regulations relate to these goals?

Requiring IPv6 capabilities to be addressed in all future acquisitions of networked information technology will ensure that Federal IPv6 capabilities evolve through continuous technology refresh cycles as opposed to incurring the cost and disruption of reactive procurements and retrofits of IPv6 capabilities. In effect, the directives are meant to encourage complete and correct implementations of IPv6 in future networked IT products – just as support for IPv4 is today.

Why are there distinct 2012 and 2014 deployment deadlines?

The OMB directives identify two specific deployment milestones (2012 and 2014) that have been identified as critical steps to (a) ensure that Federal agencies are reacting to the accelerating IPv6 roll out through-out the Internet; (b) demonstrate that Federal IPv6 planning and acquisition processes can be put into action; and, (c) establish a base-line of Federal IPv6 capability that should become a "tipping point" for fostering agency-directed broad IPv6 use in scopes beyond those of the directive.

The first deployment milestone is to upgrade external (i.e. Internet) facing servers and services that are accessible to the general public to operationally use native IPv6 by the end of FY 2012. The 2012 requirement makes sure that Federal information systems are accessible to IPv6-enabled end systems on the public Internet. Major access and mobile networks have announced plans to begin connecting customers using IPv6 within the next 2 years. The industry is reacting to this situation by IPv6-enabling key Internet content sources and services in roughly the same time frames. The Internet Society's World IPv6 Day[3] on June 8, 2010 served as a Internet-wide community test and demonstration of IPv6-enabled Internet services. The 2012 requirement will ensure that Federal information systems (and their supporting network infrastructure) keep pace with these developments and remain accessible to the emerging base of IP6-connected users.

The second deployment milestone is to upgrade agency internal client applications that communicate with public Internet servers and supporting enterprise networks to support native IPv6 by the end of FY 2014. The 2012 milestone addresses how systems that only support IPv6 can access Federal information systems. The 2014 milestone addresses how Federal client applications can access public Information systems that only support IPv6. The 2014 requirement will ensure that Federal client Internet applications (and their supporting network infrastructure) will be able to access the emerging base of IPv6-connected Internet services.

The scope and timing of these two deployment requirements were carefully chosen to:

- Address specific and tangible IPv6 deployment scenarios that are emerging within the Internet.
- Focus on servers/services and client applications that support open communication with the public users/services. Such open, uncoordinated information exchanges typically benefit the most from support of ubiquitous standards and are typically provided by commercial / commodity products (e.g., operating systems, web browsers, email agents, domain name

[3] See World IPv6 Day - http://isoc.org/wp/worldipv6day/.

servers). In particular, this scope excludes most agency-specific / custom applications (e.g. that are limited to internal use, or not accessible to the public) that will require more careful agency specific planning.

- To embody a staged deployment plan for IPv6-enabled Federal network infrastructures such that other services/applications outside the scope of these requirements can leverage operational, production quality, IPv6 network services going forward.

It is planned that these requirements and milestones will bring Federal networks to the tipping point that IPv6 becomes the commodity network technology of choice for future use going forward.

How do you define what is a USG provided "public/externally facing server or service"?

The intent of the FY 2012 requirement is to ensure that any and all networked services that agencies provide to the general public over the Internet are seamlessly accessible via both IPv6 and IPv4. That is, a service that is *both* accessible external to the agency (i.e., over the Internet) and accessible to general public users.

Internal services (i.e., accessible only within an agency enterprise or intra-net) and external services that are only accessible to sites/users employing virtual private network (VPN) technologies, or to closed user groups (e.g., requiring an out-of-band establishment of a login account) are not in scope of the FY 2012 requirement.

In summary, if there is a USG provided network service that is currently available to all users of the public Internet, that service must be available to a user who only has IPv6 capabilities.

What sites, domains and services are in scope?

Typical examples of public external facing services that are within the scope of the memorandum include external web (HTTP), email (STMP) and domain name system (DNS) services; but the scope extends to any and all such public services provided or contracted by an USG agency. This includes USG network services both named under the .gov top level domain (TLD), and in other TLDs, and includes services that are entirely outsourced to commercial providers.

How do you define what USG applications "communicate with public Internet servers"?

The intent of the 2014 requirement is to ensure that public IPv6-enabled network services that are provided external to an agency, are accessible to USG users residing in their agency enterprise networks. The definitions of what is meant by "public" are the same. That is, in this case, the same service that an USG client/application is trying to access, is available to everyone on the Internet. The agency clients applications, host operating systems, and supporting networking infrastructure should be IPv6-enabled such that it is possible to establish native IPv6 end-to-end communication between client application and the external IPv6-enabled public server/service.

Typical examples of client applications that access public Internet servers/services include external web (browsers), email (mail user agents), DNS (resolvers), and their host operating systems. Messaging and social media applications that access publicly available network servers are also within scope.

In summary, if there is an IPv6-enabled external network service that is currently available to all users of the public Internet, that service must be available to an Agency network user who only has IPv6 capabilities. Of course, this requirement does not override agency policies that might restrict employee access to such services. But if such a service is permissible to access using IPv4, it must be possible to access the same service using IPv6.

IMPLEMENTATION QUESTIONS

What does it mean to "upgrade … to operationally use native IPv6" ?

The intent of the FY 2012 requirement is to upgrade public external services to support native IPv6 transport end-to-end to IPv6-enabled clients on the public Internet. The support of this service should be transparent to the end user, meaning that it should be provided with the same service name (Uniform Resource Identifier - URI) as the existing IPv4 enabled service. That is, www.agency.gov should be IPv6 enabled, not some specially named variant of the well know service (e.g., www-v6.agency.gov).

Must the IPv6-enabled service be provided on the same physical resources as their IPv4 equivalents?

While the service must logically appear to be dual stacked to the public, this does not require that the IPv6 enabled service must share the same physical resources as the IPv4 accessible equivalent. How agencies map (e.g., load balance) external service requests to internal physical resources is beyond the scope of this requirement.

Can the IPv6 services be provided by placing protocol translators in front of existing services?

For the servers and clients that are providing IPv6 access, it is required that the native operating systems/platforms be upgraded to directly support IPv6. In particular, providing this capability with IP protocol translators operating in conjunction with IPv4-only servers is not consistent with the intent of this requirement.

As noted above the intent of the requirements is for native, end-to-end / client-to-server support of IPv6. As such, agencies are strongly encouraged to make the in-scope services IPv6 accessible as soon as possible, using any suitable technique that is transparent to the end user and that provides a user experience (e.g., in terms of content, performance, reliability) comparable to IPv4 services. Note in particular, that agencies might use protocol translation techniques (e.g., protocol translating load balancers, etc) as an interim step to achieve intermediate milestones.

ACQUISITION QUESTIONS

Is there an IPv6 Federal Acquisition Regulation (FAR)?

Yes. On December 10, 2009, the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council issued a final rule amending the Federal Acquisition Regulation (FAR) to require all new information technology acquisitions using Internet Protocol (IP) to include IPv6 requirements expressed using the USGv6 Profile and to require vendors to document their compliance with those requirements through the USGv6 Testing Program. For a summary of the relevant amendments, refer to http://edocket.access.gpo.gov/2009/pdf/E9-28931.pdf. To review these amendments in their full context, refer to https://www.acquisition.gov/far/index.html.

What are the practical implications of the FAR changes?

In response to these IPv6 FAR clauses, Agency acquisition procedures, manuals and training must be updated to ensure that:

- Unless accompanied by a written waiver approved by the Agency Chief Information Officer, when acquiring information technology that includes Internet protocols:
    1. The contents of written acquisition plans must address the inclusion of IPv6 requirements documents (see below).
        - Ref. FAR 7.105 (b)(5)(iii) Acquisition Planning / Contents of written acquisition plans.
    2. Requirements documents must include appropriate technical specifications for IPv6 capabilities expressed using the USGv6 Profile (NIST Special Publication 500-267) and requirements that vendors document their corresponding offered IPv6 capabilities by submitting an USGv6 Supplier's Declaration of Conformity (SDOC) as defined by the USGv6 Testing Program (http://www.antd.nist.gov/usgv6/testing.html).
        - Ref. FAR 11.002 (g) Describing agency needs / Policy.
        - Ref. FAR 12.202 (3) Special Requirements for the Acquisition of Commercial Items / Market research and description of agency need.

Note that these new acquisition procedures should be documented in agency acquisition manuals and added to the training materials for agency acquisition and COTR responsibilities.

Is there a template that agencies should use in following the new FAR language?

The intent of the FAR language is twofold. First and foremost agencies should require that every networked IT product that is offered, include a current USGv6 Suppliers Declaration of Conformity (SDOC) (see below) reporting test results (as appropriate) from an USGv6 accredited laboratory. A product's USGv6 SDOC should cover each and every unique IPv6 stack in the product (e.g., it is

not uncommon for modern network equipment to have multiple distinct IP stacks supporting different functions for example management ports vs data ports).

As noted above, agency procurement processes should be modified to request USGv6 SDOCs for any and all networked IT acquisitions. An example standard procurement requirement might be worded as follows:

"All networked IT products that support any IPv6 capability must provide a complete and signed USGv6 Suppliers Declaration of Conformity (SDOC) (http://www.antd.nist.gov/usgv6/sdoc.html). The vendor's SDOC should address all of the IPv6 capabilities/stacks claimed for the specific product being offered and report appropriate conformance and interoperability testing results obtained from an accredited USGv6 testing laboratory."

How does the FAR change impact the definition of requirements?

The second intent of the FAR language is to encourage agencies to use the USGv6 profile as a tool for expressing specific IPv6 requirements for a given acquisition. The USGv6 profile provides recommendations for mandatory requirements for all implementations and optional capabilities that can be specified on an as needed basis. These requirements can be specified using the USGv6 Capabilities Check List (CCL) that is provided with the SDOC template, or by simply using the short hand notation for specifying IPv6 requirements as a set of named configuration options (see Appendix A of the USGv6 Profile).

An example of the latter form of expressing requirements is as follows:

- A example IPv6 requirements specification for a personal computer acquisition might be expressed by requiring demonstrated compliance to:
  - **Host: USGv6-V1-Capable+IPv4+DHCP-client+DNS-Client+ URI+Link=Ethernet**.
- A example enterprise firewall acquisition specification might be expressed as requiring demonstrated compliance to:
  - **NPD: FW+AFW** and **Router: USGv6-V1-Capable+IGW+Link=Ethernet**

Note that the notation "USGv6-V1-Capable" is short hand for all the capabilities that the USGv6 profile recommends as mandatory. Agencies that wish to deviate from those recommendations can just enumerate subset of the capabilities recommended in the profile.

- For example, the Host requirements above could be also expressed as:
  - **USGv6-V1-Host: IPv6-Base+Addr-Arch+IPsecV3+ESP+IKEv2+Mcast+IPv4+DHCP-client+DNS-Client+ URI+Link=Ethernet**.
- To modify any of the recommended requirements, simply add/drop capabilities from this list or include notes that explain additional requirements.

NOTE - Even if an agency does choose not to use the USGv6 Profile tools to express the technical requirements of an acquisition, it is expected that all acquisitions will require the submission of an USGv6 SDOC to demonstrate the quality and completeness of the IPv6 capabilities being offered. This latter point, that acquisition officers should require a USGv6 SDOC be submitted for any product that claims any level of IPv6 support, provides important consumer protection for Federal procurements of network technologies in the near to mid-term, when the completeness and quality of IPv6 implementations vary considerably through out the industry. Acquisition officers should provide USGv6 SDOCs to the technical representative for all procurements. Agency Transition Managers should also familiarize themselves with the IPv6 capabilities of the networking products being procured within their organization.

How do agencies obtain IPv6 services through the Networx contract?

To obtain IPv6 services under Networx, agencies need to submit a request for the service. For existing circuits, agencies need to check with their vendor to see if the existing circuit supports IPv6 or a new circuit is needed. If a new circuit is needed, agencies must specify IPv6 requirements with the order. There should be no additional costs for IPv6 services under Networx unless agencies need to upgrade their network devices to support IPv6.

Do agency TIC Access Providers (TICAPS) support IPv6?

Agencies serving as TICAPs should have an IPv6 network backbone and implement plans to run in a dual-stack configuration or dedicated IPv6 configuration that is capable of interfacing with, and providing transport medium for, all other internal agency networks. The TICAP should ensure that TIC access point systems using IPv6 have at least the same security capabilities as for systems using IPv4.

For additional information on the Trust Internet Connections initiative, refer to:
http://www.dhs.gov/files/programs/gc_1268754123028.shtm

Does Managed Trusted Internet Protocol Services (MTIPS) support IPv6?

The MTIPS Statement of Work, dated November 18, 2008, states the following:

"MTIPS providers shall comply with current and future regulations, policies, requirements, standards, and guidelines for Federal U.S. Government technology and cyber security, including those listed below. Contractors shall comply with new document versions, amendments, and modifications. Those most notable include minimum expectations for MTIPS specified security services identified in this SOW. After award, the contractor may propose alternatives at no additional cost to the Government that meet or exceed the provisions."

For additional information on MTIPS, refer to: http://www.gsa.gov/portal/content/104213. You may also contact GSA at 877-387-2001 or FASnetworkservice@gsa.gov.

STANDARDS AND TEST PROGRAM QUESTIONS

What standards are agencies required to follow?

The USGv6 Profile (http://www.antd.nist.gov/usgv6/) provides a framework for agencies to express user level requirements for IPv6 capabilities in networked IT products. The profile provides the mapping from user level requirements to detailed IETF standards specifications that vendors must follow. The profile also provides NIST's recommendations for which capabilities should be required to ensure the completeness, interoperability and security of forward looking USG IPv6 procurements.

How can an agency determine if an IT product complies with USGv6 requirements?

The USGv6 Testing Program (http://www.antd.nist.gov/usgv6/testing.html) establishes the infrastructure necessary to verify if an IT product meets a set of requirements that have been expressed in terms of the USGv6 profile. All procurements of networked IT should require that the vendors submit a USGv6 Suppliers Declaration of Conformity (SDOC) that is backed by conformance and multi-vendor interoperability testing results in an accredited USGv6 test lab. Such USGv6 SDOCs allow agencies to easily determine which USGv6 capabilities / requirements are supported in a given IT product.

What is the difference between lab accreditors and test labs?

The test labs are the entities that will be performing the validation of products IPv6 capabilities against the USGv6 profile requirements.

The lab accreditors are the bodies certifying the test labs 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 the testing program?

All information about the testing program can be found here: http://www.antd.nist.gov/usgv6/testing.html. In particular agencies are directed to NIST SP 500-281 USGv6 Testing Program User's Guide.

Will the 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 the biggest step towards global integration of IPv6 standards that industry has seen to date. NIST has been actively engaged with members of the IPv6 community world-wide throughout the development of the profile and testing program,

including the IPv6 Forum (world-wide consortium), the TAHI group (Japan), and the IPv6 Ready Logo program. In addition the USGv6 Testing Program has benefitted from close collaboration with several leading network industry test labs, including the University of New Hampshire Interoperability Testing Lab (UNH-IOL), ICSA Labs and Chung Hwa Telecom IPv6 Testing Laboratory in Taiwan.

The Federal government IPv6 profile is largely a "superset" of the IPv6 Ready Logo profile, and reflects the inputs of a large user base. The respective test programs have been harmonized from the outset, since the Federal government leveraged the IPv6 Ready Logo test suites, interpretations, and resolution mechanisms in the development of the USGv6 product testing program. The continued harmonization of the USGv6 and IPv6 Ready programs is a goal of all involved.

How can vendors test their products against the profile?

The USGv6 Testing Program has been operational, with standardized test methods and accredited labs since November of 2009. Many products have already completed testing. Vendors wishing to test their products should access the USGv6 Testing Program web site to review the current set of test suites and methods and select an accredited test lab to work with.

Where can I see the list of already tested products?

First and foremost, vendors should be ready and willing to provide their USGv6 SDOCs and corresponding capability checklists upon request. In most cases, direct contact between vendors and current/future customers is the most effective way of conveying future technical requirements and effecting change in product offerings. Federal sales representatives, can be contacted to request USGv6 SDOCs for products of interest and discuss their plans for future development of IPv6 capabilities.

The structure of the USGv6 Testing Program is that the details of when and what gets reported as a test result is left to be determined by the relationship between a vendor and their chosen accredited test laboratory. Currently, a collection/registry of USGv6 SDOCs is not maintained on any USG web site. The accredited labs, however, typically provide listings of tested products and corresponding USGv6 SDOCs for their customers. To assist in finding and browsing these test results, a page has been created on the USGv6 Testing site that provides direct access to all such lists at currently accredited laboratories.

To see the current laboratory lists of USGv6 tested products, see:
http://www.antd.nist.gov/usgv6/products.html

What other forms of testing might be required?

The USGv6 Testing Program will provide the basis for product conformance and interoperability testing. The goal of the testing program is to allow agencies to have reasonable assurance of the completeness, correctness and demonstrated multi-vendor interoperability of IPv6 products.

While the testing program addresses a large portion of the problems space, especially for relatively new implementations, there are other forms of testing that agencies might find necessary before operational deployment.

- **Performance / Scaling Testing** – The USGv6 Test Program does not, in general, address issues of performance / scaling. Agencies are encouraged to work with vendors and test labs to carefully understand the performance and scaling of IPv6 products. Many test labs conduct this kind of "best of breed" testing in addition to USGv6 conformance and interoperability testing. This issue is important because often in early implementations the performance of IPv6 protocols might not be on par with those of IPv4. Assuming that most networked IT products will support both IPv4 and IPv6, agencies could include procurement requirements such as the following to address this issue:
    - "Provide test data to document the performance / scaling properties of the products IPv6 capabilities. In particular, describe any differences in the performance / scaling properties (e.g., forwarding capacity, aggregate throughput, # of sessions supported, etc) of the products IPv6 and IPv4 capabilities."
- **Systems Integration Testing –** While the USGv6 Testing Program includes multi-vendor interoperability testing, there is no guarantee that the set of implementations randomly chosen for those tests will include all of the distinct products that comprise a given agency's networking environment. In addition, such USGv6 testing is mainly focused on individual IPv6 protocols/capabilities. As a result, agencies are encouraged to conduct systems integration testing of selected IPv6 products to evaluate their behavior in an exact replica of the agency's specific networking environment. Such a test should test IPv6 capabilities in conjunction with all of the specific applications and support systems (e.g., configuration, management, monitoring) and devices (e.g., layer 2 switching infrastructure). If USGv6 Testing is used as a pre-requisite to systems integration testing, agencies should be able to focus on the systems integration issues specific to their environment, rather than issues of basic IPv6 correctness and interoperability. It should be noted that many test laboratories are prepared to conduct such testing for specific customers.
- **Deployment Testing –** Agencies incrementally enabling IPv6 systems and services do so by connecting new and existing equipment together. Existing equipment has in many cases latent IPv6 functionality not yet turned on. For example, Linux and Windows desktop and notebook systems have had support for IPv6 for some years, hitherto not yet enabled, and will not be replaced until the appropriate – hardware or software – tech refresh date. Deployment testing is needed to ensure that the operational Agency network installation continues to provide service with the new IPv6 additions. As such, it is the final testing step following the conformance, interoperability and systems integration forms of 'isolation' testing.
- **Security Authorization –** All Federal systems require security authorization in accordance with NIST Special Publication 800-37, "Guide to Applying the Risk Management Framework to Federal Information Systems." Agencies are highly encouraged to plan ahead to ensure that security processes do not delay meeting the FY 2012 and FY 2014 IPv6 milestones.

SECURITY

What is being done to address security concerns related to implementing IPv6?

Introducing a second protocol into the operational networking environments of Federal agencies clearly must be done carefully, in a way that maintains the security and stability of Federal IT systems. Historically, there have been two key issues that must be addressed to achieve the secure adoption of IPv6: (1) education and training; and (2) the level of IPv6 readiness in network security products (e.g., firewalls, intrusion detection and prevention devices).

Training operations and engineering staff about IPv6 in general can be achieved through the many training materials and services that are commercially available. Such training should always address issues of security in IPv6 deployments. To augment what is commercially available, NIST has developed SP-800-119 Guidelines for the Secure Deployment of IPv6 (http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf), which provides specific recommendations for USG agencies.

To address the issue of the IPv6 capabilities of network security products, the NIST USGv6 Profile provides specific IPv6 capability requirements for firewalls and intrusion detection and prevention products. The USGv6 Profile refers to such products as Network Protection Devices (NPDs). The USGv6 Testing Program provides for the testing of NPDs to verify which USGv6 requirements they comply with.

How do I find out what security solutions are available for IPv6 systems?

As noted above and in the testing sections, require that firewall and IDS vendors submit USGv6 SDOCs backed by testing in an accredited lab to document which USGv6 security requirements their products comply with. To find lists of already tested products, refer to the USGv6 Testing Program web site and follow the links to the individual accredited laboratories. Most labs publish a list of their tested products.