White Oak Consulting LLC

Federal IPv6 Acquisition Recommended Best Practices

Digital Government Institute Government IPv6 Conference

August 21, 2013

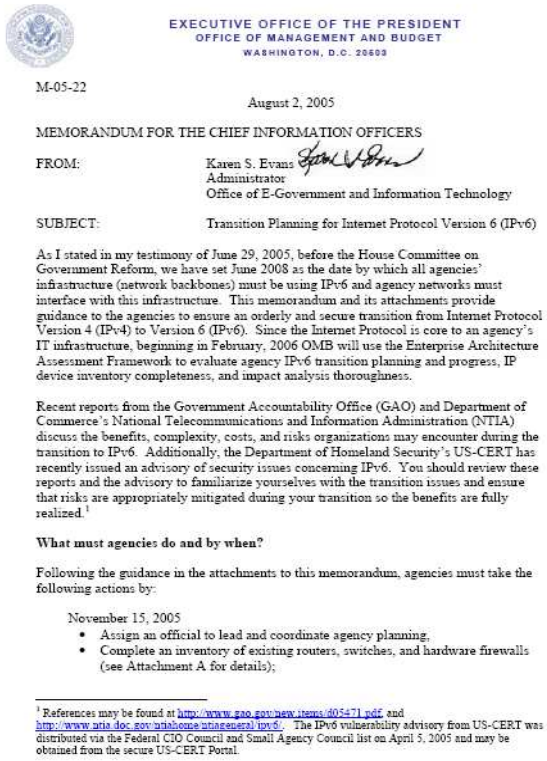
Washington, DC

Background

OMB M05-22

- Agencies: “backbone” using IPv6 by June 2008
- NIST: develop standard for USGv6 compliance
- Generate acquisition guidance

DoD, GSA, and NASA published a proposed rule in the Federal Register at 71 FR 50011, August 24, 2006, to amend the FAR to ensure that all new IT acquisitions using Internet Protocol are IPv6 “Capable”.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-05-22

August 2, 2005

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator
Office of E-Government and Information Technology

SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

As I stated in my testimony of June 29, 2005, before the House Committee on Government Reform, we have set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. This memorandum and its attachments provide guidance to the agencies to ensure an orderly and secure transition from Internet Protocol Version 4 (IPv4) to Version 6 (IPv6). Since the Internet Protocol is core to an agency's IT infrastructure, beginning in February, 2006 OMB will use the Enterprise Architecture Assessment Framework to evaluate agency IPv6 transition planning and progress, IP device inventory completeness, and impact analysis thoroughness.

Recent reports from the Government Accountability Office (GAO) and Department of Commerce's National Telecommunications and Information Administration (NTIA) discuss the benefits, complexity, costs, and risks organizations may encounter during the transition to IPv6. Additionally, the Department of Homeland Security's US-CERT has recently issued an advisory of security issues concerning IPv6. You should review these reports and the advisory to familiarize yourselves with the transition issues and ensure that risks are appropriately mitigated during your transition so the benefits are fully realized.[1]

What must agencies do and by when?

Following the guidance in the attachments to this memorandum, agencies must take the following actions by:

November 15, 2005
- Assign an official to lead and coordinate agency planning,
- Complete an inventory of existing routers, switches, and hardware firewalls (see Attachment A for details);

[1] References may be found at http://www.gao.gov/new.items/d05471.pdf, and http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/. The IPv6 vulnerability advisory from US-CERT was distributed via the Federal CIO Council and Small Agency Council list on April 5, 2005 and may be obtained from the secure US-CERT Portal.

NIST SP 500-267 A Profile for IPv6 in the U.S. Government – Version 1.0

- Acquisition Focused (not deployment, operational, etc.)
- Purpose
  - *Define a simple taxonomy of common network devices;*
  - *Define their minimal mandatory IPv6 capabilities and identify significant configuration options so as to assist agencies in the development of more specific acquisition and deployment plans; and,*
  - *Provide the technical basis upon which future USG polices can be defined.*
- Why
  - OMB Directed (05-22)
  - USG-wide benefit from a common definition of IPv6 capabilities
  - Promote confidence and protect IPv6 investments
  - "Raise the bar" of IPv6 security and network protection technologies
  - Existing profiling and testing efforts are insufficient for USG requirements
  - Support IPv6 progression to meeting future USG IPv6 requirements and protect investments

Requirements

Spec / Reference	Section	USGv6-V1 Node Requirements Title / Definition	Status	Year	Condition / Context	Host	Router	NPD	Effective Date
		IPv6 Basic Requirements							
RFC2460		**IPv6 Specification**	DS	1998		**M**	**M**		2010/07
	2	IPv6 Packets: send, receive				**M**	**M**		2010/07
	2	IPv6 packet forwarding					**M**		2010/07
	4	Extension headers: processing				**M**	**M**		2010/07
	4.3	Hop-by-Hop & unrecognized options				**M**	**M**		2010/07
	4.5	Fragment headers: send, receive, process				**M**	**M**		2010/07
	4.6	Destination Options extensions				**M**	**M**		2010/07
RFC5095		**Deprecation of Type 0 Routing Headers**	PS	2007		**M**	**M**		2010/07
RFC2711		**IPv6 Router Alert Option**	PS	1999			**M**		2010/07
RFC4443		**ICMPv6**	DS	2006		**M**	**M**		2010/07
RFC4884		**Extended ICMP for Multi-Part Messages**	PS	2007		S+	S+		
RFC1981		**Path MTU Discovery for IPv6**	DS	1996		**M**	**M**		2010/07
	4	Discovery Protocol Requirements				**M**	S+		2010/07
RFC2675		**IPv6 Jumbograms**	PS	1999		O	O		
RFC4861		**Neighbor Discovery for IPv6**	DS	2006		**M**	**M**		2010/07
	4.1, 4.2	Router Discovery				**M**	**M**		2010/07
	4.6.2	Prefix Discovery				**M**	**M**		2010/07
	7.2	Address Resolution				**M**	**M**		2010/07
	7.2.5	NA and NS processing				**M**	**M**		2010/07
(RFC4862)	7.2.3	Duplicate Address Detection				**M**	**M**		2010/07
	7.3	Neighbor Unreachability Detection				**M**	**M**		2010/07
	8	Redirect functionality				S	**M**		2010/07
RFC5175		**IPv6 Router Advertisement Flags Option**	PS	2008		S	S		
RFC4191		**Default Router Preference**	PS	2005		S+	S+		
RFC3971		**Secure Neighbor Discovery**	PS	2005	SEND	c(M)	c(M)		2010/07

Background

FAR Clauses (December 10, 2009)

- FAR 7.105(b)(4) [Acquisition Planning/Contents of written acquisition plans]

  (iii) For information technology acquisitions using Internet Protocol, discuss whether the requirements documents include the Internet Protocol compliance requirements specified in 11.002(g) or a waiver of these requirements has been granted by the agency's Chief Information Officer.

- FAR 11.002(g) [Describing agency needs/Policy]

  (g) Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. The applicability of IPv6 to agency networks, infrastructure, and applications specific to individual acquisitions will be in accordance with standards identified in the agency's Enterprise Architecture (see OMB Memorandum M-05-22 dated August 2, 2005).

- FAR 12.202(e) [Special Requirements for the Acquisition of Commercial Items/ Market research and description of agency need]

  (e) When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol compliance requirements in accordance with 11.002(g).

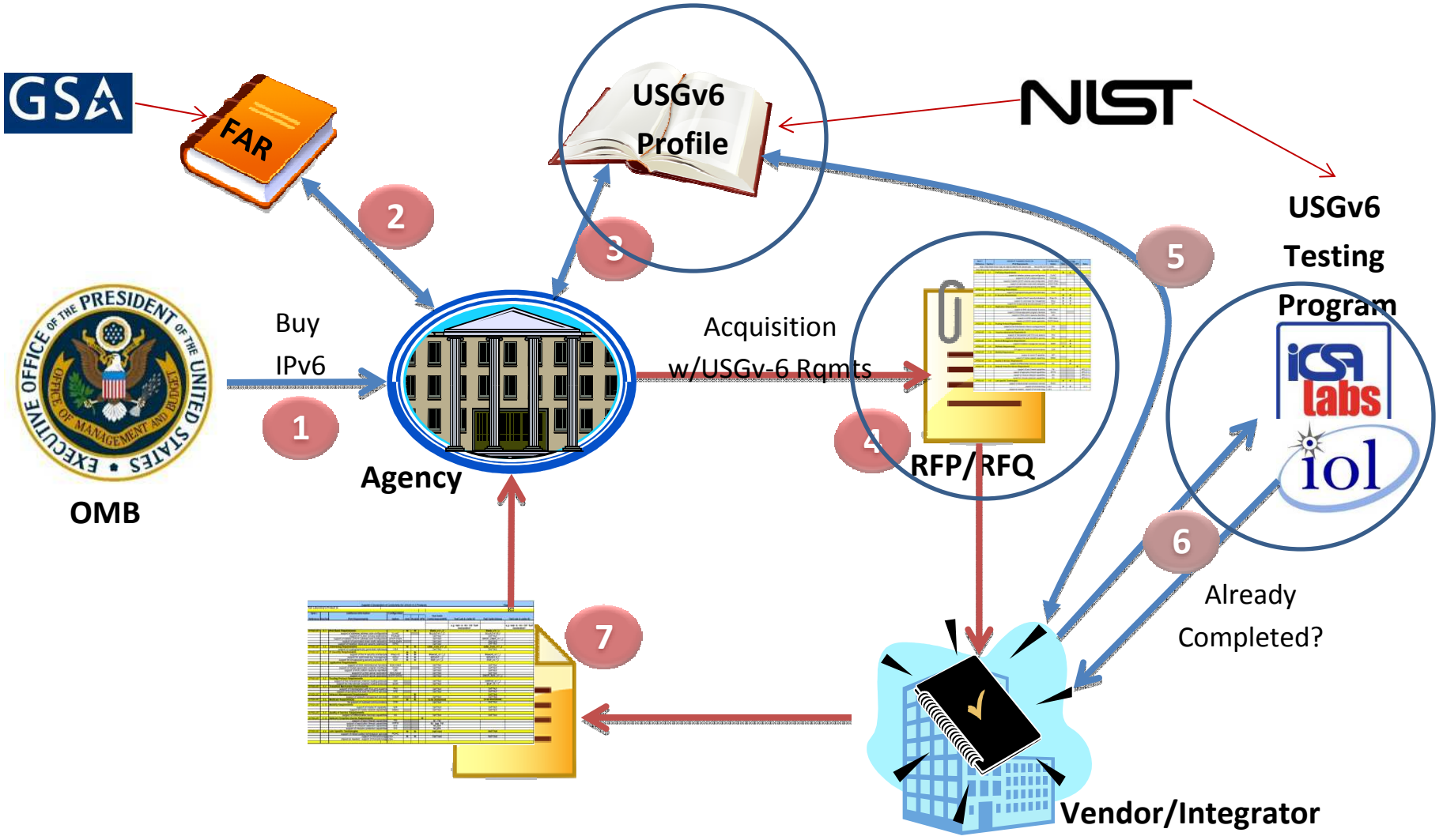
- FAR 39.101(e) [Policy]

  (e) When acquiring information technology using Internet Protocol, agencies must include the appropriate Internet Protocol compliance requirements in accordance with 11.002(g).

Federal Intent

- Provide the ability for an agency to specify what they mean when they say “I want to buy an IPv6 capable/enabled/etc product”
- Pulls from IETF RFCs (and other sources)
- Provides agency with tested products (to some degree)
  - Routers, Hosts and Security Devices
    - Conformance
    - Interoperability
- FAR focus on Agency compliance, not Vendor (no Part 52 flow down)

Workflow per FAR

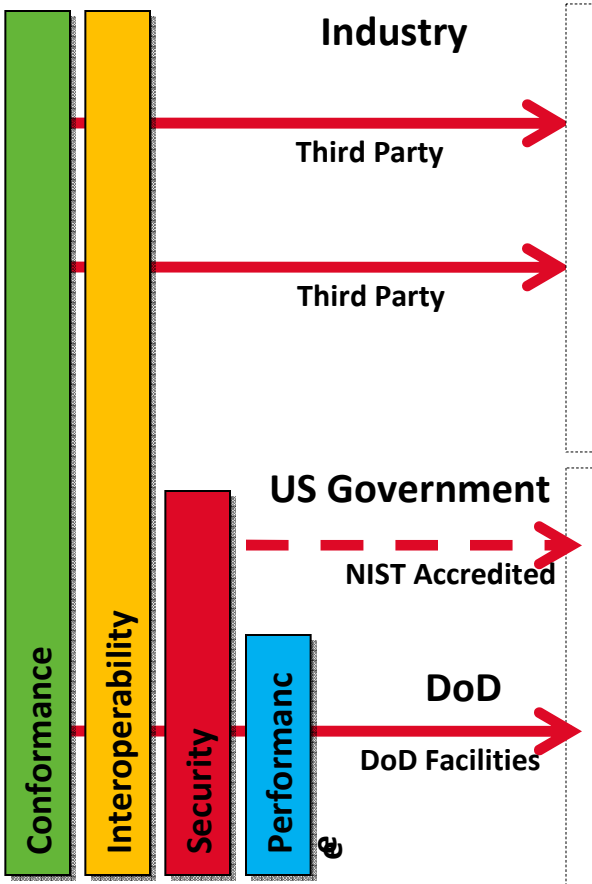


IPv6 "Capability"

Product Marketing Terms

IPv6 "Capable"
IPv6 Compliant
IPv6 Compatible
IPv6 Ready (IPv6 Task Force)
IPv6-Ready
IPv6 Available
IPv6 To Standard (IETF)
IPv6 "Enabled"
IPv6 Tested
IPv6 DoD/DISA Ready
DoD/DISA Tested
JITC IPv6 Certified

Testing



Certified

IPv6 Ready Logo Program

Phase 1
Host, Router, Special Device for minimum IPv6 Core Protocols
http://www.ipv6ready.org/logo_db/approved_list.php

Phase 2
Host, Router, Special Device for minimum IPv6 Core Protocols plus IPsec, IKEv2, MIPv6, NEMO, DHCPv6, SIP, MLD, Transition, Management(SNMP-MIBs)
http://www.ipv6ready.org/logo_db/approved_list_p2.php

USGv6 NIST Certified 1.0
Host, Router, Network Protection Devices for Routing, Quality of Service, Transition, Link Technology, Addressing, IPsec, Application Environment, Network Management, Multicasting, Mobility
http://www.antd.nist.gov/

DoD IPv6 Capable Certified 3.0
Host, Network appliances, Router layer 3 switch, Security device, Advanced server, Application
http://jitc.fhu.disa.mil/apl/ipv6.html

Any Federal Agency May institute their own IPv6 Standard, and test to that standard, to establish the Agency's IPv6 "Capable" acquisition requirements – as long as it has the USGv6 as the foundation of their standard.

Further Direction

Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government (July 2012)

3.2.2 Acquisition Guidance

It is detailed in the FAR that agency acquisition processes will be modified to include detailing of required IPv6 capabilities as defined by USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. **These processes and procedures also need to address procurement of services as well as products.**

The acquisition of IPv4/IPv6-based network infrastructure is **a collaborative effort between technical and acquisition resources, and between financial and mission management.** It is recommended that cross-functional teams be impaneled **to develop agency-specific processes and procedures addressing their requirements** that can be updated over time, as appropriate. ***These services specifications are not limited to ISP services. They may also include access methods for provision of application services, including cloud provision.***

Further Direction

Internet Protocol Version 6 (IPv6): 1 Year Check Point (OMB)

- Have you incorporated USGv6 compliant products in your acquisition planning per the FAR? What procurement artifacts do you have in place to help ensure compliance?

- Does your agency have a plan to ensure all affected agency contracts (e.g. managed web hosting services, etc.) that require modification will be modified in time to achieve the requirements of the September 2010 memorandum?

- Of the IPv6 service capabilities or equipment, software, etc. requested of vendors, were there any that they were not able to provide at this time (please explain)?

- Where your agency is dependent upon external contracts (e.g. Networx/MTIPS), has your agency communicated its requirements to the providers/vendors?

- Is your agency on track to procure all needed services and/or equipment, software, etc. in time to achieve the FY2012 and FY2014 deadlines?

IT Acquisition: Two Party Effort

Contracting Officer

- FAR Flow-Through Clauses
- Reps and Certs
- IGCE
- Trust In Negotiations Act (TINA)
- Warranties
- Source Selection Criteria

Contracting Officer's Technical Representative

- Technical Requirements to meet mission need
  - Devices/Applications
    - Capability
    - Interoperability
    - Performance
  - Service
    - Technical Capacity
    - Performance
    - Ability to meet schedule
- Trade Studies

Clinger – Cohen Act Hard Requirements regarding IT Acquisition

IPv6 Product Warranty Example

IPv6 Warranties. *The contractor warrants that each item, either hardware or software, delivered* under this contract, at the minimum requirement, shall be able to accurately transmit, receive, process, and *function correctly using the Internet Protocol Version 6 (IPv6), in accordance with the US Government IPv6 Product Profile Criteria, or, define specifically how the item is not in compliance with said profile. ……*

The duration of this warranty and the remedies available to the Government for breach of this warranty shall be defined in, and subject to, the terms and limitations of the contractor's standard commercial warranty or warranties contained in this contract, provided that notwithstanding any provision(s) to the contrary in such commercial warranty or warranties, *the remedies available to the Government under this warranty shall include repair or replacement of any product whose non-compliance is discovered and made known to the contractor in writing within one year after acceptance.*

Nothing in this warranty shall be construed to limit any rights or remedies the Government may otherwise have under this contract with respect to defects other than IPv6 performance…….

IPv6 ISP Warranty Example

The Internet Service Provider (ISP) warrants that connection service delivered to (Agency) shall be able to accurately transmit, receive, and function correctly using the Internet Protocol Version 6 (IPv6). Specifically, the ISP warrants that:

1) Their service complies with the IETF guidelines for Internet Protocol Version 6 (IPv6) Standard (RFC 2460)
2) The ISP has established IPv6 connectivity to its upstream providers and peers either directly or at Internet Exchange Points (IX)
3) The ISP can advertise routes to (Agency) IPv6 address space
4) Any additional services specified in the contract, such as multicasting support or mobility, will be compliant with the IPv6 versions of those services as specified by the IETF.
5) Service delivered is supported by the ISP's IPv6 technical support.

Additionally, as IPv6 evolves, the ISP commits to upgrading or providing an appropriate migration path for each network service delivered under this contract. The duration of this warranty and the remedies available to the Government for breach of this warranty shall be as defined in, and subject to, the terms and limitations of the contractor's standard commercial warranty or warranties contained in this contract, provided that notwithstanding any provision(s) to the contrary in such commercial warranty or warranties, the remedies available to the Government under this warranty shall include repair or replacement of any product whose non-compliance is discovered and made known to the contractor in writing within one year after acceptance. Nothing in this warranty shall be construed to limit any rights or remedies the Government may otherwise have under this contract with respect to defects other than IPv6 performance.

Acquisition Checklist

- ❑ Identify an agency lead for your IPv6 acquisition process
- ❑ Assemble a cross-agency team to support the IPv6 acquisition process development and implementation (organizations within agencies have their own criteria)
- ❑ Create an approach to developing agency specific device profiles based on the USGv6 profile (one size does not fit all; *Agencies may be more specific!*)
- ❑ Determine additional IPv6 acquisition technical requirements (USGv6 does not cover everything, especially COTS applications; *Agencies may be more specific!*)
- ❑ *Determine service offering requirements that contain IPv6 criteria (e.g. Software development, ISP, VPN, WAN, Cloud, Data Center Consolidation, Convergence, BYOD, Webhosting)*
- ❑ Determine appropriate warranty and service performance criteria.
- ❑ Document and release the process as a formal agency policy (CIO or higher memo)
- ❑ Include an IPv6 acquisition plan development checklist (like security or Section 508 compliance)
- ❑ Incorporate a quality check to make sure acquisitions are implementing the process
- ❑ Make sure your source selection teams know how to evaluate the SDOC or equivalent agency approved artifact (and other information) when they receive a proposal, in accordance with the approved acquisition evaluation criteria

Questions

How do we integrate this into our Acquisition Life Cycle?

What do we do with existing contracts?

Where do I get the funding to execute the acquisition strategy?

How do I get my executives on board?

Why am I hearing about this now for the first time?

Why don't I know if my agency is doing anything about this?

And any more questions?