DoD Internet Protocol Version 6 (IPv6) Implementation Overview

August 10, 2011

Kris Strance
Architecture and Infrastructure
Office of the DoD CIO
(703) 607-0231

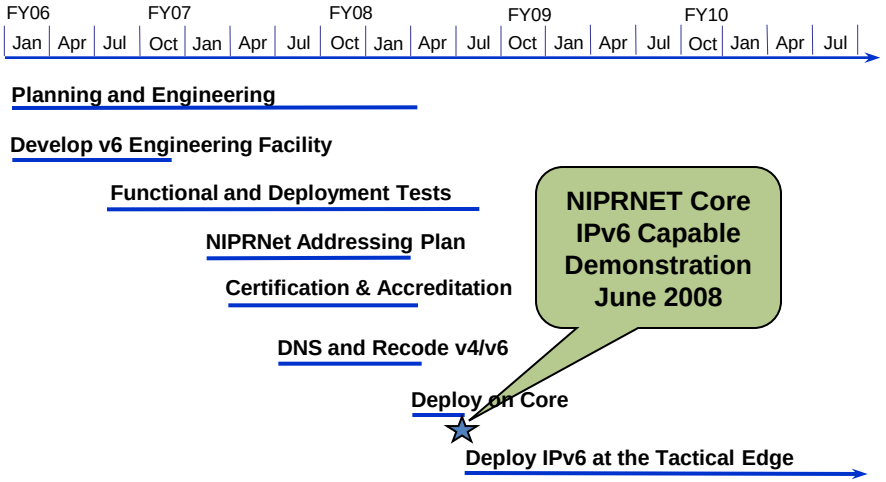
IPv6 Implementation Guidance

- **DoD CIO Memorandum -- June 9, 2003**
  - **Established goal of FY 2008 to complete the transition to IPv6**
  - **Prohibited use of IPv6 on operational networks until IA risk assessment was complete**
- **DoD CIO Memorandum -- February 6, 2004**
  - **Established DoD IPv6 Transition Office to be comprised of 10 positions**
  - **OSD to fund FY 2004 and 2005, DISA to fund FY 2006 and beyond**
- **Office of Management and Budget Memorandum -- August 2, 2005**
  - **Established June 2008 by which all federal agencies' infrastructure (network backbones) must be using IPv6**
- **ASD(NII) Memorandum -- August 16, 2005**
  - **Updated DoD transition policy contained in June 2003 and September 2003 memos**
  - **Defined Milestone Objectives for enterprise-wide deployment of IPv6**
- **DoD IPv6 Transition Plan – Provided to Congress June 30, 2006**
  - **Describes the overall DoD strategy for IPv6 transition**
  - **Identifies roles, responsibilities, and milestones**
- **Office of Management and Budget Memorandum – September 28, 2010**
  - **Describes specific steps for agencies to expedite the operational deployment and use of IPv6**

No legislative requirement for DoD to transition to IPv6
Considerable legislative interest

DoD NIPRNet IPv6 Transition

NIPRNet Transition:



Critical Path Items:

- ☑ Develop IPv6 Engineering Test Facility
- ☑ Test IPv6 6PE for Core Network
- ☑ NIPRNet IPv6 Address Plan
- ☑ Recode Address Mgt Tool
- ☑ Core Network C&A
- ☑ Conduct Core T&E
  - ☑ Deployment Test
  - ☑ Operational Test/Demo (OMB Mandate)
- ☑ Demonstrated IPv6 extension to U-AR
- ☑ Test IPv6 on STEP IA tools
- ☑ U-AR tech refresh with IPv6 capable routers

Required Funding/Resources:

- The IPv6 NIPRNet transition effort is fully funded

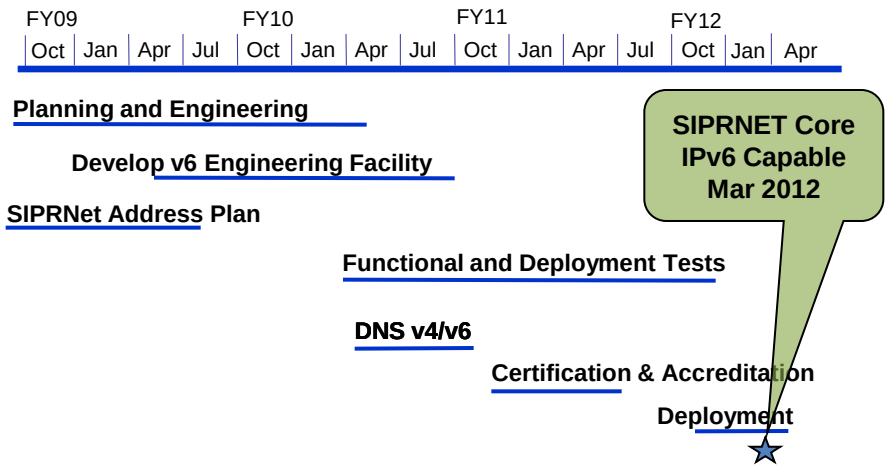
Transition Issues:

- IPv6 security device availability
- Validate IPv6 capabilities at NIPRNet/Internet boundary

IPv6 voice and video services to be tested this Summer

SIPRNet IPv6 Transition

SIPRNet Transition:



Critical Path Items:

- ☑ SIPRNet IPv6 Address Plan
- ☑ HAIPE v3
- ☐ Develop IPv6 architecture (ECD: Sep 2011)
- ☐ Conduct Core T&E
  - Deployment Test (ECD: Dec 2011)
  - Operational Test/Demo (ECD: Mar 2012)
- ☐ Conduct AR T&E
  - Deployment Test (ECD: Jun 2012)
  - Operational Test/Demo (ECD: Jul 2012)

Required Funding/Resources:

- The IPv6 SIPRNet transition effort is fully funded

Transition Issues:

- T&E of HAIPE v3 required for deployment on SIPRNet

IC and DoD Enterprise IPv6 IA Guidance

MO3 IPv6 IA Guidance

Outlines IA guidance for enterprise-wide IPv6 implementation to:

- Provide security filtering, configuration, and transition related information for IC and DoD operational network nodes in the enclave boundary, demilitarized zone, and interior environments
- **Describes best practices to assist IC and DoD personnel to mitigate security risks associated with deploying IPv6**
- Provides high-level IPv6 "IA aware" transition strategy guidance
- Augments existing network security policy with the IPv6 "missing piece"-- **not a replacement for existing security policy**
- Serves as a recommended **IPv6 IA informational reference**

IPv6 Milestone Objectives (MOs)

DoD IPv6 implementation incorporates phased IA guidance for transition:

- MO1 is authority to operate IPv6 within an isolated enclave
- MO2 is authority to operate IPv6 across multi-enclave/domain environments
- MO3 is authority to operate IPv6 in an enterprise-wide environment

MO3 IPv6 IA Guidance Summary

- **MO3 IA Guidance document jointly signed by DoD DCIO (Aug 2010) and DNI CIO (Sep 2010)**
- Intended to be incorporated into existing security policy
- **Provides flexible guidance with many prioritized alternatives to suit a wide variety of transition plans**
- Does not change existing IA C&A processes

OMB IPv6 FY 12/14 Guidance

Federal CIO Memorandum Transition to IPv6 (28 Sep 2010)

- ❑ 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 12
  - ➢ To ensure interoperability, it is expected that agencies will also continue running IPv4 into the foreseeable future
- ❑ Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 14
- ☑ Designate an IPv6 Transition Manager and submit their name, title, and contact information to OMB by 30 Oct 2010. The IPv6 Transition Manager is to serve as the person responsible for leading the agency's IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary
- ☑ Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities

---

- ☑ The Federal IPv6 Task Force met with agencies to explain the Government's IPv6 direction and to share best practices (3 Jan 2011 for DoD)
- ❑ TechStat Accountability Sessions will be led by the Federal IPv6 Task Force to ensure a timely and successful transition to IPv6

Way-Ahead
OMB IPv6 FY 12/14 Guidance

** Actions tasked in ASD(NII)/DoD CIO guidance and policy memorandum dated 7 Mar 2011*

Immediate Focus

ASD(NII)/DoD CIO Actions:

☑Issue NII/CIO guidance and policy memorandum by 7 Mar 2011

☑Submit OMB IPv6 Transition Manager Checklist and inventory of public-facing web sites by 29 Apr 2011

☑Devlop DoD IPv6 Implementation Plan for Components use by 29 Apr 2011

☑DoD participate in World IPv6 Day 8 Jun 2011

DoD Component Actions:

☑Identify public-unrestricted web sites by 31 Mar 2011

☑Identify a single Component web site to participate in initial pilot and T&E activities by 29 Apr 2011

☑Initiate T&E activities to assess Component readiness by 6 May 2011

☑NSA conduct an enterprise-wide risk assessment by 29 Jul 2011

❑Develop a POA&M to meet OMB guidance by 29 Jul 2011

Follow-on Effort:

❑Upgrade public-facing systems and security devices, appliances, and tools using certified IPv6 capable products from the DoD UC Approved Products List (APL) by 6 Jan 2012

❑Make respective public-unrestricted web, DNS, and email services available via IPv6 in the DoD DMZs or Component DMZ extensions by 29 Jun 2012

❑Eliminate public-unrestricted web sites which are no longer relevant, useful, or needed for access by the general public no later than 28 Sep 2012

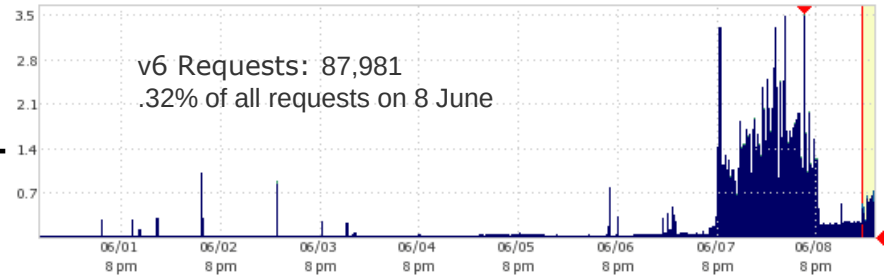
Actions Required to Meet OMB FY 14 Guidance:

- ❑ DISA, in coordination with the DoD Components, augment NIPRNet design and engineering solution(s), as required, to meet the OMB requirements
- ❑ DoD Components identify internal client applications that communicate with public Internet servers and supporting component networks
- ❑ DoD Components identify additional resources/funding required to meet the OMB requirements, and incorporate in POM FY 14 submissions

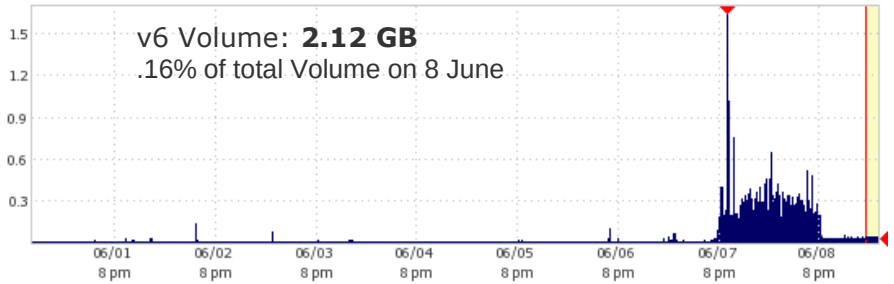
World IPv6 Day

www.defense.gov, www.af.mil, www.navy.mil

Requests



Delivered

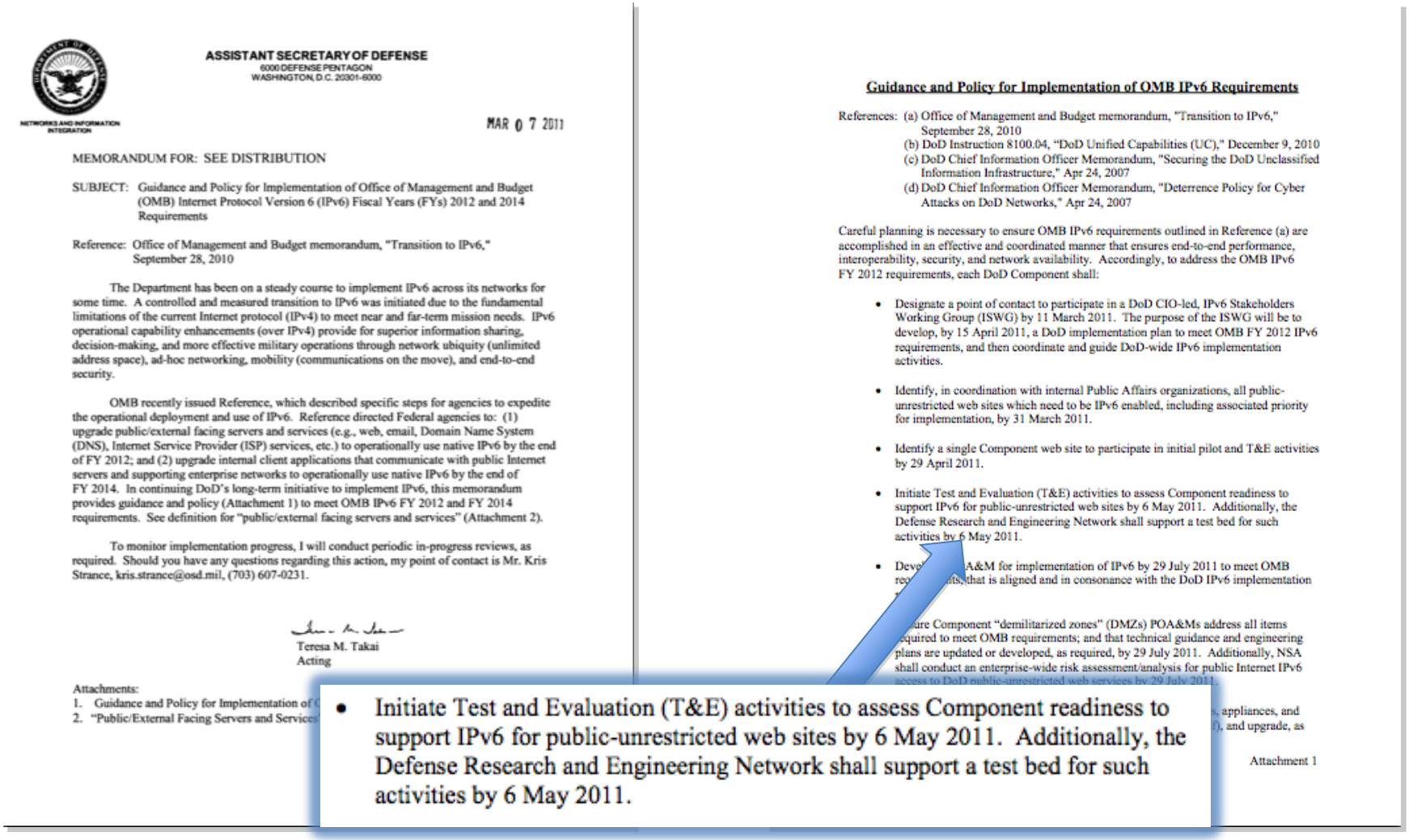


CP Code	Edge Requests	Edge Volume
All CP Codes	87,981	2.12 GB
v6 clients: ipv6/www.af.mil (121789)	20,594	0.72 GB
v6 clients: ipv6/www.navy.mil (121790)	37,223	0.46 GB
v6 clients: ipv6/www.defense.gov (121791)	30,164	0.94 GB

Notes from Kris

The message I have received from senior leadership in the services is that IPv6 is a low priority, with no operational imperative to move faster than we are, especially at the tactical edge. We will continue to build out the network infrastructure and edge devices for voice, video, and data services. Beyond that it will be the services' call as to IPv6 implementation tactically based on mission needs. We of course will continue to work to meet OMB mandates.

DoD Guidance and Policy



ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

NETWORKS AND INFORMATION INTEGRATION

MAR 07 2011

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Guidance and Policy for Implementation of Office of Management and Budget (OMB) Internet Protocol Version 6 (IPv6) Fiscal Years (FYs) 2012 and 2014 Requirements

Reference: Office of Management and Budget memorandum, "Transition to IPv6," September 28, 2010

The Department has been on a steady course to implement IPv6 across its networks for some time. A controlled and measured transition to IPv6 was initiated due to the fundamental limitations of the current Internet protocol (IPv4) to meet near and far-term mission needs. IPv6 operational capability enhancements (over IPv4) provide for superior information sharing, decision-making, and more effective military operations through network ubiquity (unlimited address space), ad-hoc networking, mobility (communications on the move), and end-to-end security.

OMB recently issued Reference, which described specific steps for agencies to expedite the operational deployment and use of IPv6. Reference directed Federal agencies to: (1) upgrade public/external facing servers and services (e.g., web, email, Domain Name System (DNS), Internet Service Provider (ISP) services, etc.) to operationally use native IPv6 by the end of FY 2012; and (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. In continuing DoD's long-term initiative to implement IPv6, this memorandum provides guidance and policy (Attachment 1) to meet OMB IPv6 FY 2012 and FY 2014 requirements. See definition for "public/external facing servers and services" (Attachment 2).

To monitor implementation progress, I will conduct periodic in-progress reviews, as required. Should you have any questions regarding this action, my point of contact is Mr. Kris Strance, kris.strance@osd.mil, (703) 607-0231.

Teresa M. Takai
Acting

Attachments:
1. Guidance and Policy for Implementation of O
2. "Public/External Facing Servers and Services

Guidance and Policy for Implementation of OMB IPv6 Requirements

References: (a) Office of Management and Budget memorandum, "Transition to IPv6," September 28, 2010
(b) DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010
(c) DoD Chief Information Officer Memorandum, "Securing the DoD Unclassified Information Infrastructure," Apr 24, 2007
(d) DoD Chief Information Officer Memorandum, "Deterrence Policy for Cyber Attacks on DoD Networks," Apr 24, 2007

Careful planning is necessary to ensure OMB IPv6 requirements outlined in Reference (a) are accomplished in an effective and coordinated manner that ensures end-to-end performance, interoperability, security, and network availability. Accordingly, to address the OMB IPv6 FY 2012 requirements, each DoD Component shall:

- Designate a point of contact to participate in a DoD CIO-led, IPv6 Stakeholders Working Group (ISWG) by 11 March 2011. The purpose of the ISWG will be to develop, by 15 April 2011, a DoD implementation plan to meet OMB FY 2012 IPv6 requirements, and then coordinate and guide DoD-wide IPv6 implementation activities.
- Identify, in coordination with internal Public Affairs organizations, all public-unrestricted web sites which need to be IPv6 enabled, including associated priority for implementation, by 31 March 2011.
- Identify a single Component web site to participate in initial pilot and T&E activities by 29 April 2011.
- Initiate Test and Evaluation (T&E) activities to assess Component readiness to support IPv6 for public-unrestricted web sites by 6 May 2011. Additionally, the Defense Research and Engineering Network shall support a test bed for such activities by 6 May 2011.
- Deve… A&M for implementation of IPv6 by 29 July 2011 to meet OMB re… nts, that is aligned and in consonance with the DoD IPv6 implementation …
- …ure Component "demilitarized zones" (DMZs) POA&Ms address all items …equired to meet OMB requirements; and that technical guidance and engineering …plans are updated or developed, as required, by 29 July 2011. Additionally, NSA shall conduct an enterprise-wide risk assessment/analysis for public Internet IPv6 access to DoD public-unrestricted web services by 29 July 2011.

…s, appliances, and …), and upgrade, as …

Attachment 1

- Initiate Test and Evaluation (T&E) activities to assess Component readiness to support IPv6 for public-unrestricted web sites by 6 May 2011. Additionally, the Defense Research and Engineering Network shall support a test bed for such activities by 6 May 2011.

Public Facing Services

- For all public facing services across all DREN customers, how many are supporting IPv6?
  - data from the DREN whitelist

web	106/1860	(5.6%)
dns	29/210	(13.8%)
smtp	28/199	(14%)
ftp	89/269	(33%)