

KEN HONG FONG - DDRE
AT&L LEAD FOR IPv6



NETWORKS AND INFORMATION
INTEGRATION

ASSISTANT SECRETARY OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

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.

A handwritten signature in cursive script, appearing to read "Teresa M. Takai".

Teresa M. Takai
Acting

Attachments:

1. Guidance and Policy for Implementation of OMB IPv6 Requirements
2. "Public/External Facing Servers and Services" Definition

DISTRIBUTION:

SECRETARIES OF THE MILITARY DEPARTMENTS

CHAIRMAN OF THE JOINT CHIEFS OF STAFF

UNDER SECRETARIES OF DEFENSE

DEPUTY CHIEF MANAGEMENT OFFICER

ASSISTANT SECRETARIES OF DEFENSE

GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE

DIRECTOR, OPERATIONAL TEST AND EVALUATION

DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION

INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

ASSISTANTS TO THE SECRETARY OF DEFENSE

DIRECTOR, ADMINISTRATION AND MANAGEMENT

DIRECTOR, NET ASSESSMENT

DIRECTORS OF THE DEFENSE AGENCIES

DIRECTORS OF THE DOD FIELD ACTIVITIES

CHIEF INFORMATION OFFICERS, MILITARY DEPARTMENTS

OFFICE OF THE SECRETARY OF DEFENSE CHIEF INFORMATION OFFICER

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.
- Develop a POA&M for implementation of IPv6 by 29 July 2011 to meet OMB requirements, that is aligned and in consonance with the DoD IPv6 implementation plan.
- Ensure Component "demilitarized zones" (DMZs) POA&Ms address all items required 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.
- Identify all impacted public-facing systems and security devices, appliances, and tools (Commercial Off-the-Shelf and Government Off-the-Shelf), and upgrade, as

required, using certified products (i.e., IPv6 capable) from the DoD UC Approved Products List (APL), per Reference (b), by 6 January 2012.

- Make respective public-unrestricted web, DNS, and email services available via IPv6 in the DoD DMZs or DMZ extensions, per References (c) and (d), by 29 June 2012.
- Identify those public-unrestricted web sites which are no longer relevant, useful, or needed for access by the general public and eliminate these sites no later than 28 September 2012.

To support implementation of OMB IPv6 FY 2014 requirements:

- DISA shall, in coordination with the DoD Components, augment NIPRNet design and engineering solution(s), as required to meet the OMB requirements.
- DoD Components shall identify internal client applications that communicate with public Internet servers and supporting component networks.
- DoD Components shall identify additional resources/funding required to meet the OMB requirements, and incorporate in Program Objective Memorandum FY 2014 submissions.

“Public/External Facing Servers and Services” Definition

All networked services, without access controls, that DoD currently provides, or will provide, to the general public (all users of the public Internet). This scope extends to any and all public-unrestricted services provided by or contracted by or entirely outsourced to commercial providers by the DoD. Internal services (i.e., accessible only within the DoD enterprise or intranet) and DoD external services (i.e., accessible from the public Internet) that have some form of access control are not within the scope of this definition. Examples of public/external facing services that are within scope include external web (HTTP), email (SMTP), and authoritative Domain Name System (DNS) services. Only DoD-provided public-unrestricted network services that are currently available to all users of the public Internet must be available to an Internet user with only IPv6 capabilities.