DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

FEB 0 6 2008

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS, MILITARY DEPARTMENTS

SUBJECT: DoD Internet Protocol Version 6 (IPv6) Implementation

References:
(a) DoD CIO Memorandum, Internet Protocol Version 6 (IPv6), June 9, 2003
(b) Office of Management and Budget (OMB) Memorandum, M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6), August 2, 2005
(c) DoD Internet Protocol Version 6 Transition Plan, Version 2.0, June 30, 2006
(d) Department of Defense Internet Protocol Version 6 Integrated Implementation Schedule, Version 1.0, October 4, 2007
(e) Department of Defense Internet Protocol Version 6 Master Test Plan, September 26, 2006

Reference (a) established the goal of transitioning DoD networks to IPv6 by Fiscal Year (FY) 2008. Further, reference (b) requires Federal agency core networks to be IPv6 capable by June 2008. Reference (c) refined DoD's IPv6 transition objectives to focus on transitioning DoD core network infrastructures by 2008. Transition of DoD networks to IPv6 is required now due to the fundamental limitations of the current Internet Protocol (IPv4) in meeting near and long-term networking requirements of the

DoD. DoD has committed to Congress and OMB that it will meet the IPv6 mandate. This will require a dedicated and cooperative effort by all DoD Components to achieve this objective.

IPv6 will enable DoD to prepare for current and future required operational capabilities. IPv6 capability enhancements (over IPv4) will provide for superior information sharing, decision-making, and more effective military operations through network ubiquity (unlimited address space), scalability, globally routable addresses, network support of Quality of Service (prioritization of voice, video and data packets), enhanced plug-and-play (ad-hoc networking), mobility (communications on the move), auto-configuration, improved multicast, end-to-end security, and improved network management. IPv6 is the critical enabler for net-centric operations to support the warfighters. Moreover, without continued DoD commitment to implement IPv6, the pace of U.S. commercial innovation and product developments will languish.

The DoD's strategy is to transition key core network infrastructures to IPv6 first, while providing a coherent and timely transition to IPv6 across the DoD that ensures performance, interoperability, and security; then focus on non-core networks, programs, and applications. The Department has synchronized IPv6 transition efforts by consolidating and integrating implementation schedules for DoD backbone networks, Military Department (MILDEP) core networks, non-core networks, and key programs (reference (d)). It is DoD's objective that NIPRNet be the first DoD core network to transition to IPv6 in 2008, with SIPRNet to follow when sufficient numbers of High Assurance IP Encryptors (HAIPE) are available to allow for transition. Additionally, the intent is to apply lessons learned from NIPRNet to the SIPRNet transition.

DoD-wide transition to IPv6 requires planning and resourcing across all DoD Components. Valuable IPv6 planning and Test and Evaluation (T&E) have been accomplished to date. While technology refreshment will cover the vast majority of the costs associated with transition of DoD core networks and programs, there are additional resources needed for sustainment of transition offices, engineering, integration, and T&E activities, which cannot be satisfied by this strategy. More emphasis is still required in the areas of IPv6 address management; T&E of core networks, IPv6 security devices, and Joint Staff IPv6 Operational Criteria; and development of information assurance guidance. To effectively prioritize IPv6 resources and efforts across DoD, and meet the OMB 2008 mandate for NIPRNet transition to IPv6, the following actions are required:

- A common definition and understanding for the term "IPv6 capable" is needed. Accordingly, the Office of the DoD Deputy CIO and the Defense Information Systems Agency (DISA) shall develop an "IPv6 capable" definition in coordination with the DoD Components by February 29, 2008.

- DoD Components shall reprioritize funds necessary to meet FY 2008 and FY 2009 IPv6 transition requirements to support respective network and program implementation schedules. Updated IPv6 implementation schedules shall be provided to DISA, for consolidation and integration, not later than March 15, 2008.

- MILDEPs, DISA, and NSA have previously committed (per reference (e)) to complete T&E of specific Joint Staff IPv6 Operational Criteria to support both NIPRNet and SIPRNet IPv6 transition, as well as the Chairman of the Joint Chiefs of Staff's certification of IPv6 parity (with IPv4) to Congress. MILDEPs, DISA, and NSA shall reprioritize funds, as required, to meet FY 2008 and FY 2009 IPv6 T&E obligations. Additionally, DISA shall consolidate and analyze DoD Component IPv6 T&E results and provide draft report to ASD(NII)/DoD CIO not later than August 31, 2008, for further submission to Congress by September 30, 2008.

- DoD Components shall include IPv6 transition resource requirements in POM submissions for FY 2010 and beyond.

- MILDEP CIOs, DISA, and NSA shall provide quarterly updates on IPv6 transition milestones, progress, and required/programmed resources, and spend plans to the DoD CIO Executive Board.

Thank you for your continued support to this effort. My point of contact for this action is Mr. Kris Strance (Office of the Deputy CIO), (703) 607-0249, kris.strance@osd.mil.

John G. Grimes