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

June 9, 2003

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
COMPONENT ACQUISITION EXECUTIVES

SUBJECT: Internet Protocol Version 6 (IPv6)

Reference: DoDD 8100.1 Global Information Grid Overarching Policy, September 19, 2002

This memorandum provides DoD policy for Enterprise-wide deployment of IPv6. Currently, Internet Protocol version 4 (IPv4) represents the mandated internetworking protocol for the DoD. The achievement of net-centric operations and warfare, envisioned as the Global Information Grid (GIG) of inter-networked sensors, platforms and other Information Technology/National Security System (IT/NSS) capabilities (ref a), depends on effective implementation of IPv6 in concert with other aspects of the GIG Architecture.

IPv6 is the next generation network layer protocol of the Internet as well as the GIG, including current networks such as NIPRNET, SIPRNET, JWICS, as well as emerging DoD space and tactical communications. Implementation of IPv6 is necessary due to fundamental limitations in the current IPv4 protocol that renders IPv4 incapable of meeting long-term requirements of the commercial community and DoD. IPv6 is designed to overcome those limitations by expanding available IP address space to accommodate the worldwide explosion in Internet usage, improving end-to-end security, facilitating mobile communications, providing new enhancements to quality of service, and easing system management burdens. Furthermore, IPv6 is designed to run well on the most current high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and without experiencing a significant decrease in capacity on low bandwidth systems.

While the precise timing and speed of commercial deployments utilizing IPv6 are uncertain, it is expected to replace IPv4 over the next several years. The significant installed base of IPv4 technology worldwide will likely result in an extended transition period where both protocols coexist. Therefore, a transition to IPv6 presents DoD with a number of opportunities and challenges that must be addressed through an overall enterprise transition strategy. The IPv6 transition across DoD will consider operational requirements, information assurance and costs, while maintaining interoperability within the Department, across the Federal Government, among our allies, and with coalition partners in addition to the civilian and commercial sectors. This overall strategy will be part of the GIG integrated architecture, appropriately recognizing Federal level initiatives and in concert with industry and international standards-making bodies. This memo provides the guidance to ensure that a DoD transition occurs in an integrated, timely and effective manner.

The DoD goal is to complete the transition to IPv6 for all inter and intra networking across the DoD by FY 2008. To enable this transition it is DoD policy for all Information Technology (IT) and National Security Systems (NSS) which make up the GIG (ref a) that:

- As of October 1, 2003, all GIG assets being developed, procured or acquired shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems/capabilities). This explicitly includes all acquisitions that reach Milestone C after October 1, 2003. The next version of the Joint Technical Architecture (JTA) will reflect this requirement.

- Segments of the GIG will complete transition over the time frame from FY 05 to FY 07. These segments and their transition dates will be specified as part of the planning process described herein.

- Specific near-term IPv6 implementation pilots, demonstrations, and testbeds will be identified by the DoD CIO within 30 days as part of the transition planning process described herein. These pilots will be designed to build confidence in facilitating the overall DoD transition to IPv6. DoD Components and Services shall undertake and participate in these activities in an aggressive manner.

- No implementations of IPv6 shall be permitted on networks carrying operations traffic within DoD at this time. This is consistent with the initial results of the information assurance risk assessment of IPv6 security implications done by the Information Assurance Panel of the Military Communications Electronics Board. These implementation guidelines are considered temporary and, in order to meet the above stated goals, will be reconsidered as part of the IPv6 transition plan.

- The Defense Information Systems Agency (DISA) shall acquire IPv6 address space sufficient to meet DoD's five year estimated requirements and initiate acquisition of IPv6 addresses to meet all future DoD requirements by September 30, 2003.

- DISA shall continue to manage DoD IP address allocation, registration and control on an enterprise basis to promote interoperability and security. DISA is the DoD Central Registration Authority (CRA) for assignment and registration of Internet Protocol (IP) address space for any and all DoD sponsored data networks and systems. DISA shall establish and maintain an effective program for accurate management and accounting of all DoD-owned IP addresses. As part of this requirement, DISA shall work with Components and Services to establish an IPv6 address-space and naming convention schema by December 30, 2003.

- DoD users will only acquire IP address space originating from DISA.

- Finally, the DoD CIO will lead, in consultation with the Joint Staff and with the participation of DoD Components and Services, the development of a draft IPv6 transition plan within one month from the date of this memo with completion of the plan within three months from the same date. The IPv6 transition plan for DoD will include:

  - Recommended transition strategy, which includes milestones and criteria for transition of legacy, upgraded, and new IP-based capabilities and systems.
  - Means for adjudicating potential Component claims that a particular GIG asset should not or cannot be transitioned to IPv6 in the timeframes noted above.
  - Recommended technical strategy that supports, for a limited period of time, the coexistence of IPv4 and IPv6.
  - Identification of what needs to be done to ensure readiness for transition, and of the required resources, organizational roles and responsibilities. This includes the early identification of specific implementation pilots necessary to reduce transition risk.
  - Identification of additional policy guidance needed.

The ASD (NII)/DoD CIO focal point for this effort is Ms. Marilyn Kraus, who can be reached at (703) 607-0255 or marilyn.kraus@osd.mil.

John P Stenbit

John P. Stenbit