ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

August 16, 2005

NETWORKS AND INFORMATION
INTEGRATION

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
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Internet Protocol Version 6 (IPv6) Policy Update

References: (a) DoD CIO Memorandum, Internet Protocol Version 6 (IPv6), June 9, 2003
(b) DoD CIO Memorandum, Internet Protocol Version 6 (IPv6) Interim Transition Guidance, September 29, 2003
(c) DoD Internet Protocol Version 6 (IPv6) Transition Plan, March 24, 2005

This memorandum updates policy provided in references (a) and (b), and defines Milestone Objectives (MOs) for enterprise-wide deployment of IPv6. Additional guidance may also be found in the DoD IPv6 Transition Plan (reference (c)) which: describes the overall strategy for IPv6 transition; identifies DoD Component roles and responsibilities; and establishes the initial planning foundation for more in-depth efforts. This plan is a "living document" and will be updated as required. A copy of this plan may be obtained from the DoD IPv6 Transition Office.

2005 SEP 16 7:47

A key tenet of the DoD IPv6 transition strategy is to minimize costs by ensuring that the products and systems acquired after October 1, 2003 are IPv6 "capable." IPv6 "capable" is defined as a system or product capable of receiving, processing and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Criteria to be considered IPv6 capable are: conformant with the IPv6 standards profile contained in the DoD IT Standards Registry (DISR); maintaining interoperability in heterogeneous environments and with IPv4; commitment to upgrade as the IPv6 standard evolves; and availability of contractor/vendor IPv6 technical support. The DoD IPv6 Transition Office has also developed an IPv6 specification (draft) which describes the functional capabilities required for each IPv6 MO. The IPv6 specification will be available through the DoD IPv6 Transition Office as it becomes finalized.

IPv6 MOs have been established to provide a controlled transition to IPv6 and are defined at the attachment. This milestone objective approach first permits use of select IPv6 pilots in an enclave environment, then expands use of IPv6 in cross/multi-domain environments. IPv6 pilot implementations will demonstrate IPv6 functional capability; and provide operational experience and lessons learned. Pilots will be selected and coordinated to demonstrate well-defined operational objectives. Guidance for submitting pilot nominations, pilot selection criteria, pilot implementation plan requirements, and timelines for pilot implementations will be provided by separate memorandum.

MO1 represents the first milestone objective in the DoD IPv6 transition, and the first instance that IPv6 traffic will be permitted in operational environments. MO1 provides the DoD Components authority to use IPv6 within an enclave (as described in the attached MO1 definition). The primary objective of the MO1 is risk mitigation, while permitting IPv6 pilots to demonstrate functional capability and build expertise for a DoD-wide transition. Pilot programs electing to enable IPv6 at MO1 must meet MO1 requirements described in the Attachment.

Reference (b) provided interim guidance for waiver submission for programs not transitioning to IPv6 by FY 2008. Henceforth, IPv6 waivers are not required by DoD CIO policy. The requirement for waivers will be reconsidered as future milestone objectives are defined. DoD Components may establish their own policy requirements for waivers. DoD Components are requested to inform the DoD CIO of their respective waiver policies.

For more information, the points of contact for this action are Mr. Kris Strance (DoD Deputy CIO Office), (703)607-0249, kris.strance@osd.mil and CDR Mark Harvey (DoD IPv6 Transition Office), (703)882-0636, mark.harvey@disa.mil.

Linton Wells II
Acting

Attachment:
IPv6 Milestone Objectives

cc:
Chief Information Officers, Military Departments

IPv6 Milestone Objectives

Current DoD policy does not allow IPv6 on networks that carry operational traffic until potential security vulnerabilities are understood and risk mitigated. Milestone objectives have been established to authorize transition to IPv6, in a step-wise approach, as IA issues are resolved. Additional milestone objectives may be defined, as required. Definitions of these milestones (MO1, MO2, and MO3) are provided below.

Milestone Objective 1 (MO1): MO1 represents the date by which evaluation of the IPv6 protocol is sufficient, and the policy, procedures, and technical guidance have been developed to allow IPv6 to operate in a single network domain or enclave environment within operational networks. At MO1, services and agencies are authorized to operate IPv6 systems within an enclave. The single domain or enclave is such that strict access controls are maintained under a single administrative authority for IA and security policy. Information flow will be tightly controlled to prevent IPv6 packets from entering or leaving the domain. The border device shall not translate nor permit the transit of native or tunneled IPv6 packets. MO1 allows the use, familiarization, and testing of IPv6 protocol and applications for operational pilots in order to ascertain issues and derive migration strategies for this new protocol. **MO1 date is October 1, 2005.**

Milestone Objective 2 (MO2): MO2 represents the date by which the policies, procedures, and technical guidance have been developed to expand the operation of IPv6 protocol across cooperative domain boundaries, but limited to within DoD networks (no internet exchange of IPv6 packets, native or tunneled). MO2 will provide the ability to evaluate the scalability and further evaluate the IPv6 IA implications using tunneling and native IPv6 routing, as available. IPv6 traffic which crosses cooperative domain boundaries must be approved in accordance with the DISN connection approval process to ensure compliance with IA policies. Multiple certification and accreditation authorities may be involved in MO2. MO2 permits applications to test IPv6 specific end-to-end capabilities and routing schema efficiencies. Limiting operation to within DoD, and only at approved locations, reduces risk to IA and operational impacts on existing IPv4 networks. **MO2 date is October 1, 2006.**

Attachment

Milestone Objective 3 (MO3): MO3 represents the date when all policy, planning, and technical transition guidance will be provided to allow tunneled and native IPv6 traffic to exist on DoD operational networks. At MO3, the DISN and DoD Components' core IP infrastructures shall accept, route, and process IPv6 protocol traffic while providing parity to IPv4. Boundary protection, deep packet inspection, and other security mechanisms to assure IA requirements shall be available and implemented to protect the DISN. MO3 permits applications and data owners to complete operational transition to IPv6 with at least the same functionality as currently found in IPv4. **Target date for MO3 is FY 2008. The exact date for MO3 will be determined after IPv6 implementation schedules are established for the DISN and DoD Components' core IP infrastructures.**

Future Milestone Objectives: Future Milestone Objectives shall be defined, as required, to represent achievement of specific IPv6 advanced features. These dates will be event and technology driven based on the maturing nature of the protocol. The DoD IPv6 Transition Office and service transition offices shall engage with program managers to determine the need for specific advanced features to support the deployment of future systems.

Attachment