



DEPARTMENT OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

SEP 29 2003

CHIEF INFORMATION OFFICER

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 SECRETARIES OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, JOINT STAFF
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Internet Protocol Version 6 (IPv6) Interim Transition Guidance

Reference: DoD CIO Memorandum "Internet Protocol Version 6 (IPv6), June 9 2003"

As described in the reference, the DoD has established the goal of transitioning all DoD networking to the next generation of the Internet Protocol, IPv6, by Fiscal year (FY) 2008. A key tenet of the DoD transition strategy is to minimize later transition costs by ensuring that the products and systems that are procured, acquired or in development after 1 October 2003 are capable of operating in IPv6 networks (as well as maintaining a capability to operate in today's IPv4 world). Given DoD's generally long technology refreshment cycle (even for COTS) and lengthy development timelines this direction is intended to posture DoD for completing a transition to IPv6 by 2008 with minimal additional cost and impact to current capabilities.

This memorandum provides interim guidance to support the requirement to begin to procure/acquire IPv6 capable GIG assets on 1 October 2003. Additional guidance will be issued once the DoD IPv6 Transition Plan is finalized and approved. DoD Components and Services are responsible for implementing this guidance in their procurements, acquisitions and developments.

What is IPv6 Capable? An IPv6 capable system or product shall be capable of receiving, processing and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific current criteria to be deemed IPv6 capable are:

- Conformant with the JTA developed IPv6 standards profile described below
- Maintaining interoperability with IPv4 (Specifically, GIG assets being developed, acquired or procured must be able to operate on/coexist on a network supporting IPv4 only, IPv6 only, or a hybrid of IPv4 and IPv6)
- Existence of migration path and commitment to upgrade as IPv6 evolves



- Availability of contractor/vendor IPv6 technical support.

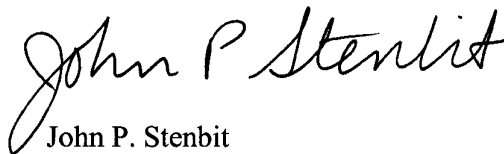
In cases where procuring, acquiring or developing IPv6 capability is not currently possible (e.g., due to lack of products or development timeline) then such acquisitions, systems or programs will be considered compliant if a funded contractual commitment to upgrade to IPv6 by the beginning of FY 2007 (or earlier if related to a DoD pilot implementation) is in place.

Alternatively, if a documented IPv6 capable technology refresh program will be fielded by the beginning of FY 2007 (or earlier if related to a pilot implementation), then the system will also be considered to be compliant.

Standards Profile: The DoD Joint Technical Architecture (JTA) Development Group formally developed an IPv4/IPv6 IT standards profile to support the direction in the reference. This profile is available at <http://jta.disa.mil/ipv6/index-public.html>. In cases where a mandated standard has yet to be identified, it is highly recommended that compliance to an identified emerging standard be considered. Concurrent action is being taken to include the standards comprising the IPv6 profile in the next version of the DoD JTA. Because of the ongoing standardization work, it is expected that this profile will be updated periodically through the work of the JTA.

Provisional Waiver Process: If the IPv6 capable criteria cannot be met, a waiver will be required. Component CIOs can waive the requirement for IPv6 capability based on consideration of the following criteria: operational need, business case, and impact on achieving GIG architecture. Component CIOs may not redelegate this waiver authority. The DoD CIO must be notified of any waivers granted and provided with the rationale ten days prior to the effective date of the waiver for final approval purposes. Finally, any waivers granted should be for one year or less, given the expected increase in availability of IPv6 capable products.

The ASD (NII)/DoD CIO focal point for this effort is Ms. Marilyn Kraus, (703) 607-0255, email: marilyn.kraus@osd.mil.



John P. Stenbit
Department of Defense
Chief Information Officer