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

May 05. 2006

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
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: DoD-wide Digital Signature Interoperability

Over the last several years, the Department has made significant progress in improving the manner in which users are authenticated to web applications and networks using the capabilities supported by the DoD Public Key Infrastructure (PKI). PKI-based digital signature capabilities are the cornerstone for transforming authenticated forms, documents and web transactions to a paperless environment.

Although current industry methods (e.g. Cryptographic Message Syntax (CMS) and Extensible Markup Language (XML)) for digital signatures are standards-based, multiple interpretations of implementing those standards by vendors mitigate against achieving true interoperability. Use of digital signature implementation profiles will minimize varying interpretations of the standards and maximize digital signature technical interoperability. This policy memorandum provides direction to incorporate the enclosed digital signature implementation profiles into all applications, systems or processes that use digital signatures. The primary targets for digital signature use are the applications and systems that require or include an authorizing or verifying signature, have auditable electronic transactions, or need to provide responsibility and traceability. Incorporating digital signature implementation profiles will improve the interoperability between digital signatures that are created and applied by disparate applications, systems and processes.

To ensure consistent digital signature interoperability and conformance, these digital signature profiles will be incorporated into the Joint Interoperability Test Command (JITC) testing regimes by the end of August 2006. Legacy systems retrofitted to use digital signature capability will also undergo JITC testing for interoperability and profile conformance. Vendor-developed digital signature applications should also be tested for compliance with the profiles.

Applications and systems with a projected fielding date after November 2006, that incorporate a digital signature capability, must ensure conformance with the profiles in their implementations at least two months prior to the projected fielding date. All other applications, systems and processes that incorporate a digital signature capability shall be JITC tested for conformance with the profiles in their implementations within three years of the approval of this memo. Waivers to the compliance requirements stated above will be handled in accordance with DoDI 8520.2.

In accordance with the timelines above, my office, in coordination with the DoD CIO Executive Board, will engage the Department's business partners to strongly encourage vendors to adhere to these profiles in current and subsequent product offerings. These profiles are intended to focus on NIPRNet applications, and will be expanded in the future to cover SIPRNet and other classified networks as PKI implementation capabilities mature.

My POC for this effort is Mr. Don Fuller, Defense-wide Information Assurance Program, donald.fuller.ctr@osd.mil, (703) 604-0500. For additional information about the digital signature implementation profiles, contact Mr. Timothy Johnson, DON CIO, (703) 602-6961 or Ms. Susan Maks, Army NETCOM IAD, (703) 602-7525.

for Priscilla E. Guthrie
Deputy Chief Information Officer

Attachment:
As stated