DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

NOV 1 0 1999

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

SUBJECT: Smart Card Adoption and Implementation

The Department is committed to innovation through the reformation of business processes and exploitation of technology to achieve our goal of efficiency and improved effectiveness. One of the Department's major initiatives in this respect has been the evaluation of smart cards for use in various operational and business applications. Now is the time to adopt smart cards throughout the Department and realize the potential that this technology offers.

Consistent with the provisions of the Clinger-Cohen Act of 1996 (Divisions D and E of Public Law 104-106), the Department's Chief Information Officer (CIO) is assigned the overall responsibility for the development of the Department's smart card policy and oversight. I direct all DoD Components to take actions necessary to implement the use of a standard DoD smart card as specified herein.

The initial implementation of smart card technology shall be effected as a Department-wide common access card (CAC). The CAC shall be the standard ID card for active duty military personnel (to include the Selected Reserve), DoD civilian employees and eligible contractor personnel. It also will be the principal card used to enable physical access to buildings and controlled spaces and will be used to gain access to the Department's computer networks and systems. This card would accommodate an integrated circuit chip and would also contain such other relevant media as magnetic stripe and bar codes. This memorandum assumes that all relevant standards will be applied to the card as appropriate. To ensure full and consistent use of existing capabilities and gain efficiencies, the CAC shall be issued and maintained using the infrastructure provided by the Defense Enrollment Eligibility Reporting System and the Real-time Automated Personnel Identification System. The DoD CIO, with the assistance of the Under Secretary of Defense (Personnel and Readiness) (USD(P&R)), is assigned the responsibility to coordinate the physical design of this new CAC using the smart card technology.

In response to the increasing threat to our networks and computer systems, I previously mandated DoD-wide movement toward a ubiquitous public key infrastructure (PKI). Since co-

U17006 /99

processor smart cards already are being used as authentication tokens for certificates and as private keys for digital signature and access authentication, the adoption of this technology within the Department--and placement on the CAC--will enable this card to serve as DoD's primary platform for the authentication token. I authorize the DoD CIO to modify previously issued PKI guidance, as appropriate, to incorporate and accommodate use of the CAC. I expect the DoD CIO to ensure an initial implementation of the smart card-based CAC at multiple locations no later than December 30, 2000. As a result of the recent Joint Requirements Oversight Council (JROC) briefing, and in support of the foregoing milestone, the Department of the Navy shall take the lead in preparing a smart card Operational Requirements Document (ORD), for submission to the JROC no later than January 31, 2000. In addition, the DoD CIO shall develop for my approval a CAC Execution Plan within 120 days of the date of this memorandum. That plan, at a minimum, shall address configuration management, a requirements planning methodology, and the use of functional community panels to ensure broad communication and cross-functional integration.

I hereby disestablish the Smart Card Senior Steering Group. In its place, the DoD CIO shall establish a Smart Card Configuration Management Control Board (SCCMCB). The SCCMCB shall assure the integration of cross-functional requirements and determine summary-level chip storage allocations, to include those for Component-specific use of the CAC. The SCCMCB will include representatives (Flag/SES minimum) from affected Principal Staff Assistants (PSAs) within the Office of the Secretary of Defense (OSD) and the DoD Components, and shall oversee the operation of a Smart Card Senior Coordinating Group (SCSCG).

An official (Flag/SES) designated by the Secretary of the Navy shall serve as the chairperson for the SCSCG. This body shall develop and implement Department-wide interoperability standards for use of Smart Card technology and a plan to exploit Smart Card technology as a means for enhancing readiness and improving business processes. This body shall accomplish these tasks by integrating smart card requirements in coordination with the DoD Components and the Public Key Infrastructure Program Management Office, and making recommendations to the DoD CIO through the SCCMCB. The SCSCG will receive technical and executive secretariat support from the Access Card Office, which currently is an element of the Defense Manpower Data Center.

The implementation of CAC applications shall be accomplished in conjunction with the OSD PSA, or designee, who is responsible for the mission or function to be supported by the CAC. Each PSA is encouraged to establish a community panel, composed of Component functional representatives, to support this role. In addition, the Military Departments and, as needed, other DoD Components, will designate organizations to serve as Component-wide smart card offices that promote and manage Component-unique smart card requirements within the chip storage allocations issued by the SCCMCB. The DoD CIO shall draft an appropriate DoD issuance to incorporate these policies and establish permanently the SCCMCB and the SCSCG.

I recognize and appreciate the efforts to date and solicit your support and cooperation as we undertake this significant effort.

John J. Hamre