DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY 6 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

SUBJECT: Department of Defense (DoD) Public Key Infrastructure (PKI)

Achieving Information Superiority in a highly interconnected, shared-risk environment requires that DoD's Information Assurance (IA) capabilities address the pervasiveness of information as a vital aspect of warfighting and business operations. To do so, DoD must provide integrated voice, video, and data transmission services that meet both warfighting and business needs as an integral part of DoD's global information enterprise. The technical strategy that underlies DoD IA is Defense-in-Depth, in which layers of defense are used to achieve our security objectives. This layering approach allows us to make use of multiple solutions of varying assurance levels and, upon failure of deterrence or prevention, to contain the consequences of a breach in security to achieve a balanced overall IA posture. This strategy recognizes the diversity of technologies, solutions, adversaries, and vulnerabilities that pervade our information systems and infrastructures. It seeks to maximize the use of COTS technology as appropriate in order to keep up with technology evolution and develop GOTS solutions only when necessary.

One element of the Defense-in-Depth strategy is the use of a common, integrated DoD PKI to enable security services at multiple levels of assurance. The DoD PKI, in the context of the Defense-in-Depth strategy, will provide a solid foundation for IA capabilities across the Department. The goal of this DoD-wide infrastructure is to provide general-purpose PKI services (e.g., issuance and management of certificates and revocation lists in support of digital signature and encryption services) to a broad range of applications, at levels of assurance consistent with operational imperatives. The Department must take an aggressive approach in acquiring and using a PKI that meets our requirements for all IA services. This policy encourages widespread use of public key-enabled applications and provides specific guidelines for applying PKI services throughout the Department.

U07287 /99

- **Selection of Appropriate PKI Certificate Assurance Levels**. To ensure consistent, proper usage of different certificate assurance levels across the DoD, effective immediately, the assurance levels of certificates issued and used for particular applications will be in accordance with the U.S. DoD X.509 Certificate Policy, as summarized below:

  - **Class 5 certificates:** Protection of classified information over unencrypted networks.
  - **Class 4 certificates:** Protection of unclassified, mission critical information (Mission Critical Systems defined at Attachment 1) over unencrypted networks. Class 4 certificates will be used to protect information crossing classification boundaries. Category 1 mission critical systems operating on unencrypted networks and employing public key technology must begin the migration to Class 4 certificates and tokens (e.g., Smart Cards, PC cards, Universal Serial Bus cards, etc.) immediately and achieve full implementation by June 2000. Near-term, this requirement can be satisfied via the FORTEZZA infrastructure.
  - **Class 3 certificates:** Protection of Category 2 and 3 mission critical systems operating on unencrypted networks must be via Class 3 certificates. These systems, that employ public key cryptography, must migrate to the use of Class 4 certificates and tokens by December 31, 2002. All other applications that employ public key technology (e.g., mission critical information on encrypted networks using NSA Type 1 approved encryption, and mission support/administrative information on any networks) must use Class 3 certificates. All DoD users will, at a minimum, will be issued a Class 3 certificate by October 2001.

- **Deployment of PKI Registration capability**. Currently there are two primary PKI efforts within the DoD: the FORTEZZA-based PKI (the near-term solution for Class 4) and the Class 3 (formerly Medium Assurance) PKI. The Department plans to leverage these two efforts and migrate them to the target PKI as defined in the DoD PKI Roadmap. However, in order to begin meeting DoD IA objectives on a widespread basis, and achieve interoperable public key cryptography within the Department as soon as possible, every DoD organization must deploy the registration capability (i.e., trained personnel and installed software/hardware for registration operations) for each of these PKIs. Every DoD organization must deploy an infrastructure having the capability to issue certificates from the Class 3 PKI to each member of the organization, in accordance with the DoD Certificate Policy, by October 2000. DoD components are currently fielding the FORTEZZA infrastructure. The user identification process must meet the trust requirements for these two certificate classes as defined in the Certificate Policy. Trust guidelines for registration will be developed by the DoD PKI Program Management Office, and coordinated Department-wide as part of the Certificate Policy.

- **Evolution of DoD certificates**. All DoD certificates will evolve to Class 4 certificates via the target PKI. As hardware token technology (e.g. smart cards, PC cards, Universal Serial Bus cards, etc.) continues to mature and becomes more interoperable and ubiquitous, DoD will evolve from Class 3 to Class 4 certificates for all applications. DoD components will begin to issue Class 4 certificates by January 2002. After this date, all Class 3 certificates that expire or must otherwise be replaced (as a result of loss, compromise, etc.) will be replaced with a Class 4 certificate. The target architecture will combine the features of an identification card, building access token, and workstation access token, on a single token. The Class 4 PKI certificate will become the common enabler for these functions.

- **The DoD PKI Certificate Types and Content**. The DoD PKI will issue identity certificates and encryption certificates. The DoD PKI will support key recovery for private keys associated with encryption certificates to support data recovery. To achieve common certificates across the entire DoD, the DoD Class 3 identity and encryption certificates will have a minimum/common set of attributes (e.g., citizenship, government/non-government employee, service, or agency affiliation). Additionally, some DoD programs (e.g. DMS) will require attribute certificates.

- **External Certificate Authorities**. To ensure secure interoperability between DoD and its vendors and contractors, interoperability will be accomplished using External Certificate Authorities (ECAs). ECAs will operate under a process that delivers the level of assurance as required to meet business and legal requirements. Operating requirements for ECAs will be approved by the DoD Chief Information Officer (CIO), in coordination with the DoD Comptroller and the OSD General Counsel.

- **Web Server Access Control via Public Key Techniques**. To improve the protection of DoD information on all private (i.e. not publicly accessible) web servers (located on classified and unclassified networks), these web servers shall, by June 2000, have at a minimum Class 3 server certificates issued by the DoD PKI. The servers shall, by the same date, use this certificate for server authentication via the Secure Sockets Layer (SSL) protocol or better. By October 2001, all private DoD and DoD-interest web servers (located on classified and unclassified networks) shall require client identification and authentication using Class 3 user certificates. Note the server/client authentication security services supported by Class 3 certificates are intended for use with clients and servers located on the same network. For access to mission critical web servers on unencrypted networks, in accordance with the *Selection of Appropriate PKI Certificate Assurance Levels* paragraph above, a Class 4 or higher certificate is required.

- **Signed Electronic Mail**. To accelerate improved protection of information exchanged within the Department, all electronic mail (as distinct from organizational messaging) sent within the Department will be signed using appropriate protocols consistent with the Department's e-mail strategy by October 2001. Department of Defense Components are encouraged to encrypt e-mail within the Department. The

certificates used for signature and encryption will be the standard identity and encryption (e.g. e-mail) certificates issued by the DoD PKI.

Implementation of these policies will ensure that DoD Components are using the infrastructure, and that future uses of public key cryptography as part of the Department's Defense-in-Depth strategy are consistent with threat and risk tolerance. The Defense-wide Information Assurance Program (DIAP), established in January 1998 by the Deputy Secretary of Defense, will provide central oversight of all DoD PKI activities. This policy memorandum will be reviewed on an annual basis, beginning January 2000, to ensure that the policy remains consistent with evolving technology and Department-wide objectives. My point of contact for this action is Mr. Richard C. Schaeffer, Jr., Director, Infrastructure & Information Assurance, 703-695-8705.

John J. Hamre

Attachment

Attachment 1
Definition of Mission Critical Systems

Mission critical systems include those systems:

Category 1: Defined by the Clinger/Cohen Act as National Security Systems (Intelligence Activities; Cryptologic Activities related to National Security; Command and Control of military forces, integral to a weapon or weapons system; systems critical to direct fulfillment of military or intelligence missions).

Category 2: In direct support of those systems identified by the Commander-in-Chiefs (CINCs) which if not functional, would preclude the CINC from conducting missions across the full spectrum of operations including:

- Readiness (to include personnel management critical to readiness)
- Transportation
- Sustainment
- Modernization
- Surveillance/Reconnaissance
- Financial/Contracting
- Security
- Safety
- Health
- Information Warfare
- Information Security

Category 3: Required to perform Department-level and Component-level core functions