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

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

April 9, 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: Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure (PKI)

Achieving Information Superiority in the highly interconnected, interdependent, shared-risk DoD environment requires that DoD's Information Assurance (IA) capabilities be applied within a management framework that considers the pervasiveness of information as a vital aspect of warfighting and business operations. 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.

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.

To ensure that the evolving DoD PKI meets the broad spectrum of mission and business needs, the DoD PKI Roadmap and DoD X.509 Certificate Policy have been updated to reflect comments received during the government and industry review process. These documents will be forwarded to addressees of this memo within one week. I am assigning program management responsibility for the DoD PKI to the National Security Agency (NSA). The Defense Information Systems Agency (DISA) will provide a Senior Executive level individual to serve as the Deputy Program Manager. Roles and responsibilities of the PKI Program Management Office (PMO), and other DoD Components, are delineated in the DoD PKI Roadmap. The PMO will provide an implementation plan for the DoD PKI Roadmap to the OASD(C3I) within 60 days of the issuance of this memorandum.

Arthur L. Money
Senior Civilian Official