COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE

ASSISTANT SECRETARY OF DEFENSE

6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

December 13, 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: Public Key Infrastructure (PKI) Operating Documents

As Deputy Secretary of Defense Hamre discussed in his May 6, 1999 memorandum, Subject: DoD PKI, 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. To create a solid foundation for the PKI program, I established the DoD PKI Program Management Office (PMO) and directed it to develop two documents that will provide operating guidance in the initial phases of implementation. These documents are: 1) The PKI Roadmap for the DoD; 2) The DoD X.509 Certificate Policy (CP). They have undergone rigorous DoD-wide review and coordination. These documents shall serve as the baseline for formulating and executing the PKI implementation strategy within the Department.

The CP provides the unified policy under which a Certification Authority and related components are to be established and operated by DoD. It also defines the creation and management of Version 3, X.509 public key certificates for use in DoD public key-enabled applications.

The Roadmap establishes the enterprise-wide end-state for the DoD PKI and outlines the strategy and timeline for the availability of PKI capabilities. The Roadmap will be reviewed and updated, as appropriate, to reflect changes in direction or strategy. The next update of the Roadmap, due within 120 days, will harmonize it with final decisions concerning the Common Access Card and Global Information Grid programs.

Approval of these documents is an essential step toward the Department's PKI implementation. I encourage your continued cooperation in this vitally important effort.

Arthur L. Money