

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

May 11, 1998

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
DIRECTOR, INTELLIGENCE SYSTEMS BOARD

SUBJECT: Secret and Below Interoperability (SABI) Reaffirmation

On March 20, 1997, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)) signed a memorandum that provided guidance for the sharing of appropriate information among users and interconnecting systems/networks at Secret levels with users and systems/networks down to the Unclassified level. The memorandum also required that all Secret systems connected to systems at a lower level of security classification be identified and validated through the SABI process by September 30, 1998.

Since the issuance of that memorandum, the Department of Defense (DoD) has made significant progress in bringing Secret and below security implementations into compliance. Successful execution of the SABI process, achieved in concert with the implementation of Department of Defense Instruction 5200.40 (*DoD Information Technology Security Certification and Accreditation Process*), has fostered community awareness and accountability for shared risk, and has resulted in reliable secure solutions for the warfighter.

The DoD is becoming increasingly reliant on globally networked information systems to perform its operational missions and daily management functions. The SABI process provides an integrated, comprehensive, and consistent approach to addressing the shared risk nature associated with high interconnectivity among networks.

Sustained leadership in implementing the SABI process is vital to ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of our information and information systems. Accordingly, the guidance and deadline stipulated in the ASD(C3I) memorandum of March 20, 1997, remain in effect. Individually and collectively, we must ensure that the implementation of the SABI process is both timely and successful.

Arthur L. Money
Senior Civilian Official