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

COMMAND, CONTROL,
COMMUNICATIONS, AND
INTELLIGENCE

NOV 4 2002

11-13-02A11:26 RC

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: Suspension of Access to Classified Information Due to Abuse or Misuse of Government Charge Cards

The Charge Card Task Force established last March by the Under Secretary of Defense (Comptroller) investigated the Department's charge card programs and recommended ways to strengthen the procedures and internal controls. One of the Task Force's recommendations is that investigative agencies must ensure that security managers and supervisors are appropriately notified when a government purchase or travel charge cardholder comes under investigation for charge card misuse or abuse.

Prompt action is required in response to allegations of charge card misuse or abuse by Department of Defense (DoD) military or civilian personnel. The commander or head of the organization has the authority (per subparagraph C8.1.3. of DoD 5200.2-R) to suspend the individual's classified access. Therefore, DoD Component security officials shall immediately report such allegations to the appropriate commander or head of a DoD organization. The commander or head of the organization shall take immediate action upon receipt of information that raises serious questions as to the individual's ability or intent to protect classified information or execute sensitive duties. The commander or head of the organization shall make an immediate determination to either to continue the individual's security status unchanged or to suspend an individual's access to classified information or assignment to sensitive duties until the appropriate authority designated in Appendix 5 of DoD 5200-2-R makes a final determination regarding the individual's eligibility to retain a security clearance.

Financial responsibility and trustworthiness are key components for determining whether a military member or civilian employee is eligible for the issuance of, or continuation of, a security clearance. These same factors should be carefully considered should instances of abuse or misuse of a government purchase or travel card be alleged. Supervisors and security managers must consider whether suspension of the individual's access to classified information is appropriate based on the applicable security standards and the specific conduct of the individual.

John P Stenbit

John P. Stenbit