POLICY FLASH 2007-06

POLICY FLASH 2007-06

DATE: November 9, 2006

TO: Procurement Directors

FROM: Office of Procurement and Assistance Policy, MA-61
Office of Procurement and Assistance Management

SUBJECT: **Improved Cyber Security Protection for Classified Computer Systems**

SUMMARY: This Flash transmits information provided by the Deputy Secretary regarding the protection of classified computer systems for internal and external threats.

Background:

Recent events at the Los Alamos National Laboratory suggest that existing efforts to secure DOE's computer systems must be enhanced. Since March 2003, the DOE Cyber Security Management Program (DOE Order 205.1), consistent with the Federal Information Security Management Act of 2002 (FISMA), requires protection of all cyber information and information systems. The Act requires, among other things, information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems.

What is the purpose of this Policy Flash?

This Flash distributes the Deputy Secretary's memo making you aware of expanded protections to be implemented as part of the DOE security revitalization effort prior to the issuance of the new cyber security Order (draft DOE Order 205.1A), which is in final review. Contracting officers must (on or before November 15, 2006) instruct and monitor affected contractors under your cognizance in their conduct of an immediate and

thorough examination of the adequacy of their practices and procedures to ensure that classified information is protected, with implementation of revised cyber security improvement steps by January 15, 2007.

What must the Contracting Officer do?

1. Ensure that DOE laboratory and facility contracts involving the operation of a classified computer system include the Contractor Requirements Document (CRD) for DOE Order 205.1, Cyber Security Management Program, and add the requirements of the attached Deputy Secretary memorandum not later than November 15, 2006.

2. Instruct DOE laboratory and facility contractors, in accordance with the guidance above, to

(a) initiate a thorough examination of the adequacy of their practices and procedures to ensure that classified information is protected using multiple layers of cyber security protection and addresses defenses against potential insider threats and inadvertent transfers of classified data;

(b) report back through the DOE Undersecretary's management chain on or before November 15, 2006 on this thorough examination; and

(c) submit a final report by January 15, 2006 that includes any steps planned or taken to ensure systems are adequately secured against insider and outsider threats, which at a minimum will include those in the attached guidance, to be incorporated in a forthcoming revision to the DOE Classified Information Systems Security Manual (DOE M 471.2-2).

3. Report on the completion of the actions above (negative responses included) not later than Thursday, November 16 to michael.fischetti@hq.doe.gov.

Additional information regarding Cyber Security may be obtained from Carl Staton, OCIO. He can be reached on (202) 586-0166 or e-mail at carl.staton@hq.doe.gov.

Questions concerning this Policy Flash should be directed to the undersigned at (202) 287-1330 or Denise P. Wright at (202) 287-1340 or Denise.Wright@hq.doe.gov

Michael P. Fischetti, Director
Office of Procurement and Assistance Policy

Attachment