The Deputy Secretary of Energy
Washington, DC 20585

November 8, 2006

MEMORANDUM FOR DISTRIBUTION

FROM: CLAY SELL

SUBJECT: Improved Cyber Security Protection for Classified Computer Systems

The Federal Information Security Management Act (FISMA) requires 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. The Department of Energy (DOE) Cyber Security Management Program (DOE Order 205.1), including the associated Contractor Requirements Document, requires that all DOE cyber information and information systems – whether operated by Federal employees or by contractors – be protected commensurate with the risks they face and the magnitude of harm that could result from the loss, misuse, disclosure, or unauthorized modification of information entered, processed, stored, displayed or transmitted on/with them. Order 205.1 has been in place since March 2003.

Recent events at Los Alamos National Laboratory, however, indicate that existing efforts to secure DOE's systems need to be enhanced. Even prior to those recent events, DOE already was working on a cyber security revitalization effort, and that effort has led to a new DOE cyber security management order (Draft DOE Order 205.1A) that is in the final stages of formal review and approval. This draft Order builds on the FISMA mandate by clarifying the assignment of cyber security responsibilities and establishing clear accountability through line management for ensuring protection of information and information systems. The Department anticipates that the new Order will be finalized by the end of 2006.

In the interim, we must ensure that our cyber information and systems are properly protected. Accordingly, I expect each laboratory and DOE facility operating a classified computer system to conduct an immediate and thorough examination of the adequacy of its practices and procedures to ensure that classified information is protected using multiple layers of cyber security protection. Each examination should address defenses against potential insider threats, and not simply defenses against outsider threats and inadvertent transfers of classified data.

I require an accounting by each laboratory and other DOE facility operating classified computer systems of the steps that each has already taken, if any, and that are planned to ensure their systems are adequately secured against both insider and outsider threats. The steps to be taken are to include, at a minimum,

those in the attached guidance prepared by DOE's Chief Information Officer. This guidance will be incorporated in a forthcoming revision of the DOE Classified Information Systems Security Manual (DOE M 471.2-2).

The laboratory directors are to report on their plans and progress in this matter on or before November 15, 2006, the date of the upcoming laboratory directors' meeting. All other DOE facilities operating classified systems are to report their plans and progress in writing through their management chain by the same date. Implementation of these cyber security improvement steps is to be completed by January 15, 2007.

Each laboratory director and other operator of a DOE classified computer system is encouraged to consult with DOE's Chief Information Officer regarding appropriate technical particulars and strategies that will provide multiple layers of cyber security protection for classified computer systems and the information they contain.

Attachment

DISTRIBUTION:

UNDER SECRETARIES
INSPECTOR GENERAL
CHIEF INFORMATION OFFICER
CHIEF HEALTH, SAFETY AND SECURITY OFFICER
DIRECTOR, OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE
ADMINISTRATOR, BONNEVILLE POWER ADMINISTRATION
ADMINISTRATOR, WESTERN AREA POWER ADMINISTRATION

Attachment to Deputy Secretary's memorandum: Improved Cyber Security Protection for Classified Computer Systems

Chief Information Officer Guidance for Improving the Cyber Security Defense in Depth of DOE Classified Systems

November 2006

The critical nature of the DOE mission as it relates to national security and protecting classified information demands that we continue to review, update, and improve our multiple layers of cyber security protection, or defense in depth, for our classified systems. At a minimum, the following additional layer of cyber security protection is to be implemented for all classified systems.

All classified systems must have physical and/or software controls in place to prevent unauthorized use of physical "ports," or connection points, on these systems that are designed for writing to removable or external media. The default setting for these connection points is to be "closed" rather than "open," and they are to be opened only as needed to support required functions. Where possible, both physical and software protection of these connection points should be employed. The effectiveness of established physical and software controls must continually be tested and validated as part of system certification and accreditation.

Groups of connection points can be physically protected rather than individual connection points, such as by protecting the computer equipment in a locked cabinet or cage, even when in a limited access area, if approved by the Designated Accrediting Authority for each system. Where connection point protection would interfere with the intended use of a system, such as for supercomputer systems and for laptops used to support emergency response teams, the Designated Accrediting Authority can approve an alternative way of providing equivalent protection.