Department of Energy
Washington, DC 20585

February 22, 2007

MEMORANDUM FOR THE SECRETARY

Greg Friedman

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "The National Nuclear Security Administration's Implementation of the Federal Information Security Management Act"

BACKGROUND

The National Nuclear Security Administration's (NNSA) mission includes maintaining and enhancing the U.S. nuclear weapons stockpile, reducing global danger from weapons of mass destruction, and providing safe and effective nuclear propulsion. To achieve its mission goals, the NNSA utilizes many classified and unclassified computer networks and individual systems. Given the sensitivity of the information residing on these networks and systems, strong cyber security measures are essential for protecting operational, personally identifiable, and other critical data from compromise. In Fiscal Year 2006, NNSA officials reported that they expended just over $90 million on cyber security in an effort to protect its information technology resources.

In September 2006, as required by the Federal Information Security Management Act (FISMA), the Office of Inspector General completed its annual independent *Evaluation of the Department's Unclassified Cyber Security Program – 2006* (DOE/IG-0738), to determine whether the Department's unclassified cyber security program adequately protected its data and information systems. Specific information supporting the unclassified cyber security report was sensitive, identified vulnerabilities by site and was not, therefore, for public dissemination. Based on the September 2006 report, and at NNSA's request, we compiled this report to provide details related to specific unclassified information system vulnerabilities.

RESULTS OF AUDIT

The NNSA had implemented a number of measures designed to reduce cyber security risks and vulnerabilities, including strong technical controls and defense-in-depth measures. In spite of these efforts, we identified a number of deficiencies that exposed critical unclassified systems to an increased risk of compromise. Specifically, we found that:

- Six NNSA sites had not completed or had not adequately performed certification and accreditation of all operational information technology systems as required by Federal regulation;

ATTACHED REPORT CONTAINS
(OFFICIAL USE ONLY) INFORMATION

- Action had not been taken to ensure that systems at six sites containing Government financial information could continue or resume operations in the event of an emergency; and,

- Weaknesses in access controls, configuration management, and change controls designed to protect computer resources from unauthorized modification, loss, or disclosure of information initially reported in 2005 had not yet been resolved.

Cyber security weaknesses have been a continuing challenge for NNSA. We found that NNSA did not always properly implement its own guidance as well as Departmental and Federal cyber security requirements. In addition, NNSA had not performed regular monitoring activities essential to evaluating the adequacy of cyber security program performance. As a consequence, NNSA's unclassified information systems and networks and the data they contain remain at risk of being compromised, including the possible unlawful diversion of operational data, personally identifiable information, or other critical information.

As we observed during our recent *Special Inquiry Report to the Secretary on Selected Controls over Classified Information at the Los Alamos National Laboratory* (OAS-SR-07-01, November 2006), the failure to establish and enforce cyber-related controls can have significant consequences. The problems with the development and enforcement of cyber safeguards at Los Alamos, that were the subject of our November 2006 report, resulted in increased vulnerabilities that could have led to the unauthorized diversion of classified information.

To help address continuing weaknesses, NNSA has developed an automated Integrated Certification and Accreditation System which was designed to aid sites in preparing certification and accreditation packages in compliance with National Institute of Standards and Technology and Department requirements. These efforts, if properly implemented and executed could help NNSA resolve continuing cyber security weaknesses. However, more effort is needed in this critical area. Our report includes several specific recommendations intended to improve protective efforts across the NNSA complex.

MANAGEMENT REACTION

Management concurred with our findings and recommendations. In particular, management indicated that NNSA is currently in the process of updating policies, and will establish an assessment team to routinely review and evaluate the implementation of cyber security requirements at NNSA sites.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Chief of Staff
Chief Information Officer, IM-1
Director, Policy and Internal Control Management, NA-66

ATTACHED REPORT CONTAINS
(OFFICIAL USE ONLY) INFORMATION