DOE F 1325.8
(08-93)
United States Government Department of Energy

Memorandum

DATE: January 31, 2007 Audit Report Number: OAS-L-07-06

REPLY TO
ATTN OF: IG-34 (A06TG041)

SUBJECT: Evaluation of the "Office of Science's Implementation of the Federal Information Security Management Act"

TO: Under Secretary for Science, SC-1

INTRODUCTION AND OBJECTIVE

To accomplish its mission of delivering discoveries and scientific tools that transform the understanding of energy and matter and advance national economic and energy security, the Office of Science (Science) utilizes numerous information systems. Given the importance of the information maintained by Science, a strong cyber security program is essential for protecting its operational, personally identifiable, and other sensitive data from compromise. In Fiscal Year 2006, Science expended over $14 million of the Department's $295 million cyber security budget 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, September 2006) to determine whether the Department's unclassified cyber security program adequately protects data and information systems. Because specific information supporting the unclassified cyber security report are generally considered sensitive and not for public dissemination and as requested by Department officials, we compiled this report to provide details related to specific vulnerabilities. We initiated this evaluation to determine whether Science's unclassified cyber security program adequately protected data and information systems.

CONCLUSIONS AND OBSERVATIONS

Over the last few years, Science has implemented a number of measures to improve its management of cyber security risks and vulnerabilities. For instance, in 2004, Science's Office of Information Technology Management, in conjunction with the Office of Independent Oversight began conducting field site visits – known as Site Assistance Visits (SAVs) – to help identify and resolve cyber security problems. These SAVs were designed to identify gaps in compliance and improve policies, procedures, and processes at each site to ensure alignment with

FISMA and National Institute of Standards and Technology (NIST) requirements. During our 2006 review at five Science field sites included in the SAV process, we noted that progress had been made in strengthening the cyber security program and improving the level of compliance with Federal directives and standards.

While the efforts were significant, our evaluation revealed problems with certification and accreditation, risk assessments, contingency planning, and security controls. We also noted that Science's Program Cyber Security Plan (PCSP) revision had not been completed as requested by the Department's Office of Chief Information Officer.

Certification and Accreditation

During this year's evaluation, we found that four sites had not completed or adequately performed all required certification and accreditation (C&A) activities. For example, Fermi National Accelerator Laboratory (Fermi) had not completed the C&A process for its general support systems and other major applications, including the Mass Storage System. Prior to our field work, a SAV had been conducted and Fermi began to modify its C&A documentation to comply with NIST guidance. At three other sites (Lawrence Berkeley National Laboratory (Berkeley), Oak Ridge National Laboratory (ORNL), and Argonne National Laboratory (Argonne)), specific detailed activities required by guidance promulgated by Science and NIST had not been performed or had not been documented. Based on our testing, we noted that:

- Accreditation boundary information at Berkeley and ORNL lacked sufficient detail to identify all system components and determine the scope of certification and accreditation. These two sites had not documented system boundaries for any of the systems included in our review.

- Security plans were incomplete or missing critical elements at two sites. Specifically, some of ORNL's security plans were not signed by officials and did not document system interconnections. In addition, Argonne's individual certification packages lacked documentation of risk assessments and security plans that laid out each group of systems' operational differences and risks, including system interconnections and controls specific to the applications and systems.

- At three sites, evaluation and testing of information systems security controls for accreditation of systems either had not been adequately performed or had not been documented. In particular, Argonne lacked individual certification packages that contained documentation of system control testing and evaluation for controls specific to system groups. At ORNL, security controls testing and evaluation was not performed in accordance with the controls outlined in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Systems.* Although various system tests were run for ORNL's groups of systems, these did not include testing of minimum security controls recommended for a system as outlined in NIST SP 800-53. Finally, at Berkeley none of the systems had documented security control test plans.

- At Berkeley, annual self-assessments had not been performed for any of the six systems included in our review. Self-assessments, required annually by FISMA, provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish targets for improvement.
- Finally, ORNL had not performed a system-specific risk assessment for any of its three enclaves.

Subsequent to our review, officials at Fermi and Argonne informed us that corrective actions had been initiated. According to officials at Fermi, the site's Chief Information Officer had completed the documentation required for the C&A process and a review of this documentation was started by an independent expert. Also, Argonne indicated that it plans to conduct an independent assessment by June 2007 to meet the evaluation and testing of security controls requirement. The remaining sites indicated that they would begin corrective actions.

Risk Assessments

Although most Science sites reviewed had performed risk categorization assessments, three sites had not performed these assessments in accordance with NIST requirements. These sites (Oak Ridge Office (Oak Ridge), Chicago, and Fermi) used a broad grouping or "enclave" approach to complete C&A of its systems and grouped low risk systems with those requiring higher protection levels. Particularly, information systems at these sites were inappropriately assessed as low impact; however, the systems contained information that inherently required a higher level of protection. Oak Ridge and Chicago assigned a security categorization of low for its general support systems – a rating which did not properly reflect the moderate or high impact level of risk for supported application systems. In spite of NIST guidance to the contrary, Fermi assigned a security level category of low for a major application. A lower security category could potentially affect the selection, implementation and testing of security controls used to protect Federal financial information and resources. Officials at Oak Ridge and Chicago indicated that corrective actions had started.

Contingency Planning

Five Science sites – Chicago, Argonne, Berkeley, Oak Ridge, and ORNL – had not taken the action necessary to ensure that their systems could maintain or resume critical operations in the event of emergency or disaster. Specifically:

- Contingency plans for systems at Chicago lacked a documented sequence to restore systems and system components in the event of a service interruption or disaster.

- Testing of contingency plans was not performed at four sites – Berkeley, ORNL, Oak Ridge, and Argonne. At Berkeley, testing was not performed for any of its six systems. Oak Ridge and ORNL each had not performed testing for at least one of their systems, Information Resource Management Division at Oak Ridge and Enterprise Resource Planning System at ORNL. In addition, Argonne had not tested the contingency planning for any of the three systems we reviewed.

- Individual systems located at Argonne lacked documentation of disaster recovery plans.

Without adequate contingency and disaster recovery planning, recovery from unforeseen and unplanned events could delay restoring critical operations or potentially lead to the loss of sensitive information. Each of the sites above stated that corrective actions were underway or would be initiated shortly.

Security Controls

Weaknesses in security controls were identified at four Science sites during this year's evaluation. Controls in this area consist of configuration management and access controls designed to protect computer resources from unauthorized access, which could lead to modification, loss, or disclosure of data. At Chicago and Oak Ridge, we found outdated or unpatched versions of application and operating system software. Also at Chicago, we noted weak or easily guessed passwords for system access that were not in compliance with Departmental policy. These vulnerabilities were resolved immediately after identification, and as such, were not reported as weaknesses needing corrective action in our *Evaluation of the Department Unclassified Cyber Security Program – 2006* (DOE/IG-0738, September 2006).

Similar to our findings, the Office of Independent Oversight found weak patch and password management enforcement at two other Science sites, Ames Laboratory and Stanford Linear Accelerator Facility. Without adequate management of security controls, there is an increased risk of unauthorized access.

SUGGESTED ACTIONS

Science is moving forward in improving its cyber security management with its expansion of the SAV program and planned revision of the PCSP. We encourage Science to release their updated PCSP as soon as reasonably possible to provide direction to all Science sites consistent with current Federal requirements. Specific recommendations were provided to field sites to correct deficiencies noted during our evaluation. To enhance its cyber security improvement efforts, we suggest that the Under Secretary for Science require responsible officials to:

(1) Ensure that the C&A process for assessing and selecting the security categories is appropriate for the protection of Federal financial resources in compliance with NIST requirements; and,

(2) Ensure that deficiencies noted in contingency planning and security controls are corrected in a timely manner.

Since no formal recommendations are being made in this report, a formal response is not required. We appreciate the cooperation of your staff during this audit.

Rickey R. Hass
Assistant Inspector General
for Financial, Technology, and Corporate Audits
Office of Audit Services
Office of Inspector General

Attachment

cc: Audit Liaison Team, SC-32.1
Program Analyst, Office of Security Assistance, HS-81

Attachment

SCOPE AND METHODOLOGY

The audit was performed between February 2006 and January 2007 at several Office of Science (Science) locations. To accomplish the audit objective, we:

- Reviewed applicable laws and directives pertaining to cyber security and information technology resources such as Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130 (Appendix III), and the Department of Energy (DOE) Order 205.1;

- Reviewed applicable standards and guidance issued by National Institute of Standards and Technology (NIST);

- Reviewed Science's overall Cyber Security Program management, policies, procedures, and practices throughout the organization;

- Assessed controls over network operations and systems to determine the effectiveness related to safeguarding information resources from unauthorized internal and external sources; and,

- Evaluated selected field sites in conjunction with the annual audit of the Department's Consolidated Financial Statements, utilizing work performed by KPMG LLP (KPMG), the Office of Inspector General (OIG) contract auditor. OIG and KPMG work included analysis and testing of general application controls for systems as well as vulnerability and penetration testing of networks.

We also evaluated Science's implementation of the *Government Performance and Results Act* and determined that it had established performance measures for unclassified cyber security. We did not rely solely on computer-processed data to satisfy our objectives. However, computer-assisted audit tools were used to perform probes of various networks and drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests.

This evaluation was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We discussed the contents of this report with a Science representative on January 11, 2007.