U.S. Department of Energy
Office of Inspector General
Office of Audit Operations

Evaluation Report

The Department's Unclassified Cyber Security Program - 2004

DOE/IG-0662

SEPTEMBER 2004

Department of Energy
Washington, DC 20585

September 24, 2004

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department's Unclassified Cyber Security Program - 2004"

BACKGROUND

In Fiscal Year 2004, the Department of Energy (Department) estimated it would spend about $2.7 billion on information technology to support its various missions. As a leader in scientific and experimental computer development and utilization, the Department deploys numerous networks and thousands of individual information systems that meet day-to-day mission requirements such as finance, security, and, research and development. As with other Government and private sector organizations, the Department faces a growing threat of intrusion or damage to its mission critical systems. External experts now calculate that, on average, a system that is not properly protected will be compromised by hackers or malicious individuals within 20 minutes after it is exposed to the internet.

In 2002, the *Federal Information Security Management Act* (FISMA) was enacted to encourage agencies to develop and maintain adequate cyber security controls to protect information resources from the increasing number of cyber threats. As required by FISMA, the Office of Inspector General conducts an annual independent evaluation to determine whether the Department's unclassified cyber security program adequately protected data and information systems. This memorandum and the attached report present the results of our evaluation for Fiscal Year 2004.

RESULTS OF EVALUATION

The Department continues to improve its unclassified cyber security program. The Office of the Chief Information Officer has issued a series of new cyber security policies that address previously reported weaknesses. We found that these polices also emphasize a risk-based approach to managing security, that, when fully implemented, should strengthen cyber security across the Department. In addition, the Department has initiated a campaign to certify and accredit its major applications and general support systems and has also improved its cyber security incident reporting. While these actions are commendable, problems continue to exist in the Department's unclassified cyber security program that, if uncorrected, could expose critical systems to compromise. We observed that the Department had not completed implementation of a comprehensive risk management program. Specifically, the Department had not:

- Completed certification and accreditation of each major system to identify and mitigate risks;

- Prepared contingency plans to ensure that mission critical systems could continue or resume operations in the event of an emergency or disaster; and,

- Ensured adequate security controls were in place at all of its sites. Specifically, we observed continuing problems with ensuring that only authorized individuals could access information resources, duties and responsibilities for processing financial transactions were properly segregated, and that known security vulnerabilities were corrected.

As reported in the evaluation for 2003, the Department's continued difficulty in identifying, tracking, and correcting previously reported weaknesses in a timely manner contributed to the remaining cyber security issues. For example, the Department closed findings prematurely, in part, because it did not require supporting evidence to verify that the weakness had actually been corrected. Despite outreach efforts and the publication of detailed guidance by the Chief Information Officer, we also noted that site level information technology professionals did not fully understand the Department's cyber security requirements. As a result, a number of unclassified information systems and networks remain vulnerable to attack. The potential for harm is demonstrated by the frequency of successful intrusions, 199 in the last year, affecting 3,531 systems across the complex. Without continuing vigilance in this area, it is likely that future attacks will continue to jeopardize the availability and integrity of critical information technology assets.

To its credit, senior-level Departmental management officials have focused their attention on improving cyber security posture. We noted that the Deputy Secretary had engaged senior officials in the process and had initiated an aggressive campaign to complete certification and accreditation of all major applications and general support systems. These actions are promising, and, when coupled with existing initiatives, should help ensure that the Department continues to improve its readiness in this important area. We have made several recommendations designed to supplement these initiatives and improve the overall effectiveness of on-going efforts.

Due to security considerations, information on specific vulnerabilities and locations has been omitted. Management officials at the sites evaluated have been provided with detailed information regarding identified vulnerabilities, and in some instances, have initiated corrective actions.

MANAGEMENT REACTION

Management generally concurred with our findings and recommendations. Where appropriate we incorporated Management's comments into the body of this report.

Attachment

cc: Deputy Secretary
Under Secretary for Energy, Science, and Environment
Administrator, National Nuclear Security Administration
Chief of Staff
Chief Information Officer

EVALUATION REPORT ON THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM - 2004

TABLE OF CONTENTS

Cyber Security Program

Appendices

Program Improvements

Our evaluation established that the Department of Energy (Department) had taken steps to strengthen its cyber security program and implemented countermeasures to reduce network vulnerabilities addressed in our *Evaluation of the Department's Unclassified Cyber Security Program-2003* (DOE/IG-0620, September 2003). Specifically, the Chief Information Officer (CIO) has issued several policies that, if effectively implemented, should improve cyber security throughout the Department. Additionally, the Deputy Secretary initiated a campaign to complete certification and accreditation of the Department's major applications and general support systems. The Department also acted to improve its reporting of cyber security incidents. Finally, the number of cyber security weaknesses we identified during our evaluation continued to decline, from a high of 69 in 2002 to 32 in FY 2004.

Cyber Security Policies

During the period under evaluation, the CIO issued several policies to address previously reported weaknesses. These policies were designed to improve the Department's security posture and included requirements for:

- Use of wireless devices and information systems, such as personal digital assistants and cellular phones;
- Certification and accreditation of all major applications and general support systems to ensure data and information systems are appropriately secure and operating at an acceptable level of risk;
- Remote access to Department and contractor information systems; and,
- Implementation of a risk-based approach to managing cyber security and the mandatory use of the National Institute of Science and Technology (NIST) methodology for evaluating computer security.

Focus on Certification and Accreditation

During FY 2004, the Deputy Secretary initiated a campaign to conduct certification and accreditation (C&A) on all of the Department's major applications and general support systems. C&A enables program officials or system owners to, among other things, develop policies and procedures to address high-risk issues through cost-effective mitigation strategies. The Office of the

Chief Information Officer (OCIO) took the lead on the C&A initiative and required program offices to certify and accredit 90 percent or more of their systems by June 30, 2004. To accomplish this objective, the OCIO established milestones and issued several data calls to the program offices. The OCIO required the programs to submit accreditation statements to support the successful completion of C&A for their systems.

Incident Prevention, Warning, and Response

The Department had also made progress in improving its incident reporting problems outlined in our report on the *Implementation of Indications, Warning, Analysis and Reporting Capability* (DOE/IG-0631, December 2003). In response to the report's recommendations, the Department finalized its inventory of sites that should be reporting cyber security incidents and now requires monthly reporting from all components. Additionally, the Department issued interim policy that includes requirements for negative reporting. The interim policy also requires Departmental elements to certify monthly, in writing, that all reportable incidents that occurred during the previous calendar month had been reported to management. The incident reporting policy is in the final stages of review and the Department expects it to be issued in late September or early October 2004.

While these actions are positive, the Department needs to update security plans to address cyber security incident reporting, establish performance goals to fully satisfy FISMA requirements, and to complete actions on our earlier recommendations. These activities, when finalized, should help to ensure that the Department provides timely notices regarding cyber attacks.

Risk Management and Control Procedures

Although the Department continued to make improvements to its cyber security program during the last year, we noted that additional work is needed to ensure that a comprehensive risk management program is completed. The risk management process provides the framework for managing threats to agency operations, assets, and employees resulting from the operation of an information system. Specifically, the Department has not completed necessary action in the C&A and contingency planning areas. Additionally, the Department continued to experience cyber security control problems in the areas of access controls, segregation of duties, and configuration management.

Certification and Accreditation

In spite of the Department's campaign, at the time of our review 4 of the 25 sites we evaluated had not completed C&A on all of its major and general support systems. While program officials currently report that work has been completed for over 90 percent of the Department's systems, we noted that some of the systems were operating under interim approval because they had not satisfied all C&A requirements. Additionally, the Government Accountability Office's (GAO) recent review of the Department's C&A process noted difficulties in determining the risks accepted by authorizing officials in the accreditation decision or the length of time the accreditation was in effect.

In a recent discussion regarding our draft report, we learned that the OCIO had initiated steps to validate the C&A process and had completed validation reviews of several packages for systems operating at Headquarters. The CIO also told us that she had asked program offices to provide copies of all system accreditation letters, including both interim and final authorities to operate, to her office. The CIO stated that these validation reviews, which included a review of accreditation letters, identified problems in the C&A process. The responsible program offices have been directed by the Deputy Secretary to correct those problems.

Contingency Planning

Five of the 25 sites included in our review had also not taken adequate action to ensure that they could maintain or resume critical operations in the event of emergency or disaster. Specifically, the Department had not developed contingency or disaster recovery plans for financial systems at two sites or tested existing contingency plans at another three sites. For example, we found one contingency plan for a financial application that did not contain documented procedures for testing the plan. Specifically, the contingency plan did not include important areas of test planning, test results, and corrective actions, key steps needed to identify flaws in the plan and its implementation. Additionally, we found that another contingency plan was in development, however, it was missing a risk assessment and had not been finalized.

Access Controls

The Department continues to experience access control weaknesses across the complex. Strong and functional access controls are essential for ensuring that only authorized individuals have access to information resources. Access controls consist of both physical and logical controls designed to protect computer resources from unauthorized modification, loss, or disclosure. We found that 7 out of 25 sites reviewed during our evaluation had cyber security weaknesses related to networks, systems, or applications, including:

- Passwords did not always comply with Departmental policy. For example, vendor default passwords were not changed in two instances. Since vendor default passwords are widely known, malicious individuals could exploit them to gain access to sensitive information;
- Excessive system administrator access privileges were granted at two sites, including an instance where temporary administrator access had not been revoked. These privileges, if exploited, could permit unauthorized or malicious modifications to systems or information;
- Documented procedures were not in place at two sites to ensure that account access was removed in a timely manner when employees were terminated;
- Periodic reviews to determine whether unauthorized use had occurred were not conducted at two sites; and,
- One site granted network access to certain students and visitors without performing mandatory background checks.

We also found instances of physical access deficiencies at two sites' primary data centers, including unlocked doors, unsecured media, access by non-data center employees, and audit logs that were not regularly reviewed.

Segregation of Duties

Our review disclosed several instances of inadequate segregation of duties. Such controls are important because they inhibit fraudulent activities by controlling personnel activities through formal operating procedures, supervision, and review. Specifically, we found:

- An employee in a financial systems group had the ability to enter invoices and then authorize them for payment, a practice that if exploited, could result in erroneous, unauthorized or fraudulent transactions;

- Eight employees who could establish employee records and create payroll records for the same individuals, increasing the chance that an individual could establish and pay non-existent employees; and,
- Computer programmers who could make system program changes and place them into the production environment, thus increasing the risk that individuals may create, and put into production, improper, unauthorized, or malicious program modifications.

Configuration Management

Our testing also revealed configuration management weaknesses at five sites we visited. Essential to a coordinated and strong security policy, configuration management controls help to ensure that computer applications and systems are controlled and protected against unauthorized modifications. While the Department corrected several problems that were reported last year, we found similar problems this year at different sites. For example, we noted:

- Despite the availability of vendor supplied updates, known software security vulnerabilities had not been corrected;
- Ineffective planning, testing, and follow-up that caused security patches designed to prevent known computer viruses and exploits to fail when deployed; and,
- Undocumented procedures for system changes that could potentially result in inconsistently applied processes and lead to compromise of the system.

Correcting and Identifying Weaknesses

Weaknesses persisted because the Department has not ensured that organizations properly identified, tracked, and corrected previously identified cyber security weaknesses. Despite outreach efforts and the publication of detailed guidance by the Department's OCIO, we also noted that site level information technology (IT) professionals were not always cognizant of the Department's cyber related policies.

Plan of Action and Milestones

In spite of prior year recommendations, the Department did not always maintain and update its Plan of Action and Milestones (POAM) database and establish it as the authoritative management tool to identify and track agency actions for correcting cyber security weaknesses. While the Department had made some progress in improving the accuracy of its POAM database since our last evaluation, our review found that 9 of 47 uncorrected cyber security weaknesses reported during our FY 2003 evaluation were not included in the Department's quarterly reports to the Office of Management and Budget (OMB). Additionally, 6 of 7 findings re-issued in FY 2004 were marked as closed or completed in the POAM database, but had not actually been corrected. Even though specifically noted in our previous evaluation, the Department continued its practice of permitting sites to close findings without providing supporting evidence or verifying that the weakness had actually been corrected.

To address this issue, the OCIO recently issued guidance to the program offices to ensure the verification that cyber security weaknesses are corrected prior to closing them. In particular, the OCIO now requires that the validation of closed findings be performed by someone other than the individual directly responsible for the correction of the weakness.

Cyber Security Awareness

The Department's efforts to promote the benefits of a robust cyber security program may not always be reaching the local levels of IT professionals across the Department. The OCIO has initiated a number of efforts to increase awareness of necessary cyber security controls, including issuing Departmental policy and guidance, hosting an annual cyber security conference, and providing training to IT professionals. However, we found that, in some cases, local IT professionals did not fully understand the Department's policy and guidance. For example, local officials did not understand requirements for C&A and password management.

Operational Impacts

Even though the Department's overall cyber security posture has improved, a number of unclassified information systems and networks remain vulnerable to attack. Failure to place proper emphasis on correcting identified weaknesses unnecessarily exposes critical information resources to threat of compromise. For example, the Department's systems and networks were recently the subject of a series of successful attacks where an external party gained broad access to multiple systems on several occasions. In addition, the Department reported that it was the subject of 199 successful intrusions during FY 2004.

As previously discussed, Government organizations face an increasing threat of intrusion or damage to their IT systems. Accordingly, the Department needs to ensure it has implemented an aggressive program of risk management and security controls to mitigate such risks.

RECOMMENDATIONS

This report identified a number of weaknesses that need to be addressed by the Chief Information Officer, in coordination with the National Nuclear Security Administration and Program Secretarial Officers. Additionally, the Department should:

1. Ensure program elements use the POAM as a management tool for cyber security by:

   a. Entering and tracking the status of corrective actions taken to close all known cyber security weaknesses; and,
   b. Verifying the effectiveness of corrective actions before closing identified weaknesses.

2. Require organizations to establish a mechanism to ensure that the Department's information technology policy and guidance are communicated and understood by cognizant cyber security officials; and,

3. Ensure that all major applications and general support systems are certified and accredited.

MANAGEMENT REACTION

Management generally concurred with our findings and recommendations. The CIO stated that C&A data was still being collected and they have initiated a process to independently verify and validate the C&A process. Based on an agreed-upon protocol, management provided informal comments to our report. Such comments were discussed with the CIO and her staff on September 15, 2004, and, where appropriate, have been incorporated into our report.

AUDITOR COMMENTS

Management's proposed actions are responsive to our recommendations.

Appendix 1

OBJECTIVE

To determine whether the Department's unclassified cyber security program adequately protected data and information systems.

SCOPE

The audit was performed between February and September 2004, at several Department locations. Specifically, we performed an assessment of the Department's unclassified cyber security program. The evaluation included a limited review of general and application controls in areas such as entity-wide security planning and management, access controls, application software development and change controls, and service continuity. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls. The Office of Independent Oversight and Performance Assurance (OA) performed a separate review of classified and national security information systems.

METHODOLOGY

To accomplish the objective, we:

- Reviewed applicable laws and directives pertaining to cyber security and information technology resources, such as FISMA, OMB Circular A-130 (Appendix III), and DOE Order 205.1;

- Reviewed applicable standards and guidance issued by NIST;

- Reviewed the Department's overall cyber security program management, policies, procedures, and practices throughout the organization;

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

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

- Evaluated and incorporated the results of other audits, evaluations, and inspections performed by the Department's OIG, OA, and the GAO in our report.

We evaluated the Department's implementation of the *Government Performance and Results Act* related to the establishment of 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 devices. 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.

The 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 our objective. Accordingly, we assessed internal controls regarding the development and implementation of automated systems. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our evaluation.

An exit conference was held with OCIO officials on September 15, 2004.

RELATED REPORTS

- *Implementation of Indications, Warning, Analysis and Report Capability* (DOE/IG-0631, December 2003). The report found that the Department had not developed and implemented a program to monitor security incident reporting and had not established performance goals to measure the success of policy implementation. While the Department implemented policy changes in response to our previous audit, they were not completely effective and did not substantially increase reporting. The Department lacked focus and quantifiable performance measures to guide day-to-day operations relating to cyber security incident reporting.

- *Management Challenges at the Department of Energy* (DOE/IG-0626, November 2003). The Department's OCIO is developing corrective actions to mitigate cyber security risks and to improve relevant controls. For instance, the Department is finalizing detailed cyber security policy and guidance, and in June 2003 provided guidance for cyber security performance measurements. Additionally, the Department recently issued DOE Order 205.1, Department of Energy Cyber Management Program, which requires that continuity of operations, configuration management, and incident reporting procedures be developed and maintained in Program Cyber Security Plans and site Cyber Security Program Plans.

- *Evaluation of the Department's Unclassified Cyber Security Program-2003* (DOE/IG-0620, September 2003). Our evaluation found that cyber security weaknesses persisted because management had not taken sufficient action to ensure that all previously identified cyber security weaknesses were properly identified, tracked, and corrected in a timely manner. The Department also had not established program-level performance metrics to guide cyber security program execution or evaluate performance. Despite OMB requirements, the Department had not always maintained and updated its POAM. Specifically, our examination revealed that 22 of 30 uncorrected cyber security weaknesses reported during our 2002 evaluation were not included in the Department's quarterly reports to OMB.

- *Inspection of Portable Electronic Device Information Security at Selected Sites* (S03IS024, September 2003). This Management Alert concerned security issues regarding the use of portable digital assistants in the Department of Energy complex.

- *Information Security: Continued Action Needed to Improve Software Patch Management* (GAO-04-706, June 2004). This audit identified, among other things, challenges to performing patch management and additional steps that can be taken to mitigate the risks created by software vulnerabilities. GAO found that agencies, including the Department, are not consistently performing risk assessments and testing all patches before deployment. However, GAO reported that agencies face several challenges to implementing effective patch management, including timeliness of patches, ensuring mobile systems receive the latest patches, and adequate resources.

- *Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation* (GAO-04-376, June 2004). GAO found that agencies, including the Department, are not consistently reporting C&A performance data. Additionally, GAO found that there are other factors that lessen the usefulness of the reported performance data, including the limited assurance of data reliability and quality and the need to refine reporting requirements to provide better information on the status of agencies' information security efforts. Further, when reviewing C&A packages from the Department, GAO found varying degrees of comprehensiveness and instances where required steps were incomplete, such as missing and/or untested contingency plans, an outdated security plan, and missing risk assessments.

- *Information Technology Management: Government-wide Strategic Planning, Performance Measurement, and Investment Management Can be Further Improved* (GAO-04-49, January 2004). The report states that Federal agencies did not always have in place important practices associated with information laws, policies, and guidance. There were also numerous instances of individual agencies that did not have specific IT strategic planning, performance measurement, or investment management practices fully in place. Agencies cited a variety of reasons for not having these practices in place, such as that the CIO position had been vacant, that not including a requirement in guidance was an oversight, or that the process was being revised.

- *Volume II, Independent Oversight Cyber Security Inspection of the Y-12 Site Office and Y-12 National Security Complex* (January 2004).

- *Volume II, Independent Oversight Cyber Security Inspection of the Sandia National Laboratories* (November 2003).

- *Independent Oversight Cyber Security Inspection of the Thomas Jefferson National Accelerator Facility* (July 2004).

IG Report No.: DOE/IG-0662

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name ______________________________ Date ________________________________

Telephone __________________________ Organization __________________________

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.doe.gov

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.