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

Evaluation Report

The Department's Unclassified Cyber Security Program-2003

DOE/IG-0620

September 2003

Department of Energy
Washington, DC 20585

September 16, 2003

MEMORANDUM FOR THE SECRETARY

Greg Friedman

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department's Unclassified Cyber Security Program 2003"

BACKGROUND

Currently, the Department of Energy spends over $2.5 billion each year on information technology to support its mission. As significant as this program is currently, the Department is increasing its focus on the electronic delivery of information and services to both internal customers and members of the public. Given its size and complexity, providing security for the Department's cyber program, both classified and unclassified, is a daunting task. On almost a daily basis, "hackers" attempt to exploit vulnerabilities and corrupt information technology resources that have become essential for virtually all aspects of the Department's mission.

In response to the continuing threat to Federal information resources, Congress enacted the Federal Information Security Management Act (FISMA) in 2002 to ensure that all agencies develop and maintain adequate cyber security controls to protect information resources. As required by FISMA, the Office of Inspector General performed its annual independent evaluation to determine whether the Department's unclassified cyber security program protected data and information systems.

RESULTS OF EVALUATION

While we noted a number of improvements in the Department's unclassified cyber security program since our last review, problems continue to exist in several critical areas. Specifically, we observed that the Department had not:

- Consistently implemented a risk-based approach to cyber security management;
- Developed or fully tested plans for maintaining or resuming critical operations in the event of an emergency or disaster;
- Resolved several previously reported problems or strengthened configuration management controls designed to protect systems from unauthorized modification or damage at nine sites;
- Corrected access control problems at five locations; and,
- Significantly improved cyber security incident reporting.

The evaluation disclosed that in many instances, the Department had not acted to identify, track, and correct previously reported issues in a timely manner. Management also had not established program-level performance metrics to guide cyber security program execution or evaluate performance. As a result, the Department's unclassified information systems remain vulnerable to attacks that may affect the availability or integrity of its information assets.

In addition to sites and systems specifically covered during this evaluation, the Office of Inspector General has done extensive work in the area of cyber security and performance management at locations throughout the Department of Energy. Where relevant, we have incorporated the results of our audits in this report, including our most recently issued report on *Security Over Wireless Networking Technologies* (DOE/IG-0617, August 2003). In addition, we have evaluated the design and implementation of performance measures in conjunction with a number of programmatic audits and the annual audit of the Department's financial statements. As a result of this body of work, the Office of Inspector General identified information security and performance management as among the most significant challenges facing the Department (*Special Report on Management Challenges at the Department of Energy* (DOE/IG-0580, December 2002).

In March 2003, under your direction, the Department initiated an aggressive campaign to mitigate the challenges included in that report. In response to this initiative, which has been personally led by the Deputy Secretary, the Office of the Chief Information Officer identified root causes and developed a plan of action to improve cyber security and mitigate the risk of harm to the Department's systems.

We also noted that the Department had taken an aggressive approach to strengthening cyber security during the past year and had implemented a number of measures designed to reduce network vulnerabilities. The Office of the Chief Information Officer had also issued or drafted a number of policies and guidelines that, when implemented, should help strengthen the Department's cyber security program. While significant progress has been achieved, additional action is necessary to correct the problems we identified. Accordingly, we have made several recommendations designed to enhance the Department's overall cyber security posture.

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.

Attachment

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

THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM-2003

TABLE OF CONTENTS

Program Management

Appendices

Program Management

While improvements were made during the last year, we noted that additional work is needed to correct problems with risk-based security management, continuity of operations, configuration management, and access controls. Despite policy changes and prompting by the Department of Energy's (Department) Chief Information Officer (CIO), sites and organizations had also not significantly improved computer incident reporting.

Risk-Based Management

We observed that certain sites had not implemented a comprehensive risk-based approach to managing cyber security. Required by both the Federal Information Security Management Act (FISMA) and Department policy, such an approach enables program officials or system owners to develop policies and procedures to address high-risk issues through cost-effective mitigation strategies. Despite these requirements, we noted that risk mitigation strategies were not adequate at 11 of the sites we reviewed. For example, we noted:

- Risk assessments that were incomplete, outdated, or had not been prepared in accordance with guidance issued by the Department and the Office of Management and Budget (OMB);
- Cyber security program and/or system plans that were missing critical elements or did not cover recent changes to the sites' information technology environment; or,
- Lack of security control reviews and management authorization to operate systems (commonly referred to as certification and accreditation) as required by OMB.

Continuity of Operations

Even though specifically required by OMB, 13 sites had not taken adequate action to ensure that they could maintain or resume critical operations in the event of emergency or disaster. Specifically, we identified a number of sites that had not developed, updated, or tested contingency and disaster recovery plans. We observed that in some situations backup storage facilities and alternative processing sites were located in close proximity to one another. While convenient, such arrangements increase the risk that common emergencies or disasters could destroy backup copies of critical business information or alternative processing facilities. Problems in this area are particularly persistent and have been previously reported in information technology and financial-related audits for several years.

Configuration Management

Our testing also revealed configuration management weaknesses at many of the sites we visited. As noted by the U.S. General Accounting Office (GAO), proper configuration management ensures that all necessary updates or patches are applied, prevents unauthorized modifications, and ensures that the implementation of changes do not result in applications or systems becoming less secure. While the Department corrected a number of previously reported problems, our testing revealed control issues at nine sites. In particular:

- Several sites did not maintain or enforce structured procedures for updates and patches to application software, operating systems, and networks;
- A network intrusion detection system was not properly configured to provide timely notifications when suspected break-ins or attacks occurred;
- At several sites, certain persons were able to perform incompatible functions such as programming and operation of the same computer system; and,
- Certain organizations did not implement or test wireless network security measures.

Access Controls

Five locations included in our evaluation had access control weaknesses related to networks, systems, or applications. Access controls consist of both physical and logical controls designed to protect computer resources from unauthorized modification, loss, or disclosure. Adequate access controls are essential for ensuring that only authorized individuals have access to information resources. Specifically, we found that:

- Passwords did not always comply with Department policy, and in one instance, were not required for network access;
- Documented procedures were not in place to ensure terminated employee and contractor account access was removed; and,
- An access control system, such as card readers, key management, or sign-in/sign-out procedures, was not in place to prevent or detect unauthorized access to computer facilities.

Cyber Security Incident Reporting

Despite efforts to strengthen policy, overall incident reporting had not improved significantly. Specifically, we observed that sites and organizations continued to have wide discretion in reporting and that in Fiscal Year (FY) 2002:

- Over half of the Department's organizations made no reports of malicious activity;
- Federal law enforcement officials were notified of only 20 of 49 successful systems intrusions;
- Site personnel did not always preserve evidence that law enforcement officials needed to investigate or determine the source of attacks; and,
- Attacks originating from foreign sources were not always reported to cognizant counterintelligence officials.

Without timely and complete reporting, the Department may be unable to prevent or detect emerging or recurring attacks and lacks critical information necessary for assessing risk.

Focus on Corrective Actions and Performance Metrics

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.

Plan of Action and Milestones

Despite OMB requirements, the Department had not always maintained and updated its Plan of Action and Milestones database (POA&M). 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. After reviewing the results of our analysis in this area, officials from the Office of the Chief Information Officer (OCIO) told us that the weaknesses were originally entered in the POA&M. However, various sites subsequently did not complete corrective actions and report on the weaknesses identified in our 2002 report. Even though these findings were issued and Department elements provided responses in Fiscal Year 2002, OCIO officials told us that the findings were never reported to OMB because program offices did not recognize them. Based on follow-up testing, we also found that two cyber security weaknesses were reported as closed but had not actually been corrected. Sites were permitted to close the findings without providing supporting evidence or verification that the weakness had actually been corrected.

Officials from the OCIO told us that the Department had initiated action designed to satisfy OMB expectations that the POA&M be used to proactively manage the Department's cyber security program. In particular, the Associate CIO for Cyber Security indicated that his office had developed a Cyber Security Scorecard to help program elements focus or prioritize needed corrective action. The Department's POA&M administrator also told us that every effort is being made to utilize the database to its full potential and that previously unreported findings would be included in the 4th quarter report to OMB.

Program Level Performance Metrics

The Department had also not established program-level performance metrics to guide cyber security program execution or evaluate performance. While the CIO has advocated adoption of program or site-specific performance metrics, organizations have been slow to adopt such measures. Such action could enhance ability to highlight the strengths and weaknesses of security controls and permit management to adjust resources to target areas of need. More importantly, measuring program performance is a key feature of the President's Management Agenda and is a requirement of FISMA. Departmental officials told us that program elements will soon be required to implement program level measures and will be able to take advantage of the National Institute of Standards and Technology's (NIST) recently published Security Metrics Guide for Information Technology Systems.

Continuing Vulnerabilities

While the Department's overall cyber security posture has improved, a number of unclassified information systems remain vulnerable to attack. The Department's information resources will continue to remain at risk until it corrects previously identified weaknesses and implements measures to guide and measure performance in this vital area. As recognized by OMB, effective remediation of information technology security weaknesses and timely incident reporting are essential to achieving a mature and sound information technology security program and securing our information and systems. As the CIO noted in recent guidance, the requirements to conduct adequate security planning and evaluate control effectiveness are not new. Failure to place proper emphasis on correcting identified weaknesses unnecessarily exposes critical information resources to threat of compromise.

Program Improvements

To its credit, we noted that the Department had taken an aggressive approach to strengthen cyber security and had implemented counter measures to reduce network vulnerabilities since our evaluation of *The Department's Unclassified Cyber Security Program 2002* (DOE/IG-0567, September 2002). In addition, the CIO has issued or drafted several policy statements that, if implemented, should improve cyber security throughout the Department, including:

- DOE Order 205.1 which revised the Department's cyber security management program;
- A series of draft cyber security policies and guidance on certification and accreditation of systems, information technology risk management, wireless technology, remote access to systems, computer virus and incident reporting, and sanitization of computer media; and,
- A memorandum emphasizing the need for a risk-based approach to managing cyber security and mandating the use of the NIST self-assessment methodology for evaluating computer security.

While significant progress has been achieved, additional action is necessary to correct the problems we identified and enhance the Department's overall cyber security posture.

RECOMMENDATIONS

We recommend that the Under Secretary for Energy, Science and Environment and the Administrator, National Nuclear Security Administration, in conjunction with the Chief Information Officer:

1. Ensure all program elements make full use of the POA&M to identify, track and ultimately correct all cyber-security weaknesses, regardless of the source;

2. Verify that all cyber security weaknesses are corrected prior to closing them; and

3. Implement a program-level cyber security metrics program to guide day-to-day operations.

MANAGEMENT COMMENTS

Auditor's Note: Because of short timeframes for reporting, the Office of Inspector General and Departmental Management agreed to an expedited comment period for this report. The following comments were based on a series of meetings between the Office of Inspector General and the Associate Chief Information Officer for Cyber Security.

Risk Management

The Department of Energy (DOE) and DOE element management have focused their efforts on the most critical systems in their inventory. System security plans and risk analysis of our systems is proceeding at a rapid pace to meet the requirements of the Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) guidelines. Training personnel and completing the documentation is a difficult and resource consuming task that DOE is committed to completing expeditiously. Peer reviews of the quality and completeness of each plan are also being conducted to verify that DOE systems have implemented the appropriate cost effective controls to minimize the risk for each system.

Configuration Management

Over the last year, DOE has deployed thousands of workstations configured to the new DOE standard. DOE understands the importance of configuration and change management and is in the process of implementing the appropriate programs while bringing current assets under configuration control. Patch management and application configuration control are also in process.

Access Controls

DOE has clearly defined access control procedures and password policies. Those responsible for granting access receive periodic and ongoing training for the proper execution of these functions. When cases that are out of the norm are brought to the attention of management they are handled on a case-by-case basis. When actions have been taken that violate DOE policy the actions are corrected and the individual(s) involved receive corrective training to ensure this does not occur again. DOE also has a clearly defined password policy. Network system administrators are trained in the proper administration of this policy. All managers and those performing verification functions verify access controls are in place on an on-going basis and when problems are uncovered they must be, and are, corrected immediately. We have multiple certification and verification functions to provide management assurance that our systems continue to operate in a secure manner.

Cyber Security Incident Reporting

The requirements for reporting will be clearly defined in the new *Incident Prevention, Warning, and Response (IPWAR*) *Manual* that will be published as guidance during the first quarter FY 2004. Management focus over the last six months has been changed to include a prevention function as well as a reactive function to past or ongoing activity. The robustness and completeness of this function is an ongoing focus of the Office of the Chief Information Officer (OCIO). As highlighted by recent guidance from FedCIRC the reporting guidance and requirements are continuously changing. DOE is committed to ensuring that appropriate information is shared to minimize the impact of intruder activities on all government systems.

Recommendation 1: Concur with Comment. The OCIO requests an official POA&M update from program elements on a quarterly basis. They may at any time during the quarter provide additional updated information. The Deputy Associate CIO for Cyber Security issues detailed instructions to the program elements for the update and provides a forum at the weekly Cyber Security Coordination Group meetings to discuss any issues or questions. Responses from all program elements are obtained and added to the POA&M prior to the quarterly OMB submission. To date, no program element has failed to respond to this data call. Although responsibility for entering and updating information lies with each program element, the OCIO facilitates this process by coordinating with them when information on new findings or weaknesses appear in published audit reports and evaluations.

Program elements are using the POA&M more and more as an overall tracking tool for all their findings. Recent direction from the OCIO requires program elements to include in their quarterly updates whether self-assessments were conducted and the results. A number of offices have already reported these data and more are expected in the future as plans for self-assessments are finalized. The OCIO will continue to require reporting of these and other internal assessments and remind program offices to fully report all findings during the next data call in December 2003.

Finally, the OCIO uses POA&M data to prepare the Cyber Security Scorecard. Quarterly, the OCIO prepares and provides to DOE senior management officials a Cyber Security Scorecard that provides information on the number of open findings and their due dates by Department and location within the Department. An analysis is prepared on the primary causes of open findings by Departmental element to help them focus on areas needing particular attention.

Recommendation 2: Concur. The OCIO through its quarterly updates, will request data on the extent to which LPSOs have verified their submissions.

Recommendation 3: Concur. On June 10, 2003, the CIO issued a memorandum for Heads of Departmental Elements specifying requirements for the quarterly reporting of Tier I performance metrics for cyber security. These metrics included OMB's overall measurement categories as well as 13 additional metrics. These departmentwide metrics are required every quarter. In addition, the memo specified that Departmental Elements must develop and use lower lever or "Tier II" metrics to measure the performance of particular areas of importance within their programs. However, until DOE O 205.1 goes into effect on September 18, 2003, Tier II metrics are not required. A sample of the Tier II metrics was provided and the Office of Cyber Security offered assistance to program elements. The OCIO will continue to require these metrics and will work with program elements, as needed, to help them structure and define useful program-level measurements. The initial data call for Tier I metrics occurred in July 2003. The next one will occur in December 2003.

AUDITOR COMMENTS

Management's proposed actions are responsive to our recommendations.

Appendix 1

OBJECTIVE

As required by FISMA and the OMB implementing guidance, the OIG performed its third annual evaluation to determine whether the Department's unclassified cyber security program protected data and information systems.

SCOPE

Between March and August 2003, we performed an assessment of the Department's unclassified cyber security program. Specifically, we assessed controls over network operations to determine the effectiveness related to safeguarding information resources from unauthorized internal and external sources. The evaluation also 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 performed a separate review of classified information systems.

METHODOLOGY

To accomplish our evaluation 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, and reviewed the Department's overall cyber security program management, policies, procedures, and practices. Selected Headquarters offices and field sites were evaluated in conjunction with the annual audit of the Department's Consolidated Financial Statements, utilizing work performed by KPMG LLP, the OIG's contract auditor. The evaluation included analysis and testing of general and application controls for systems as well as vulnerability and penetration testing of networks. To minimize duplication of effort, we directly incorporated the results of other audits, evaluations, and inspections performed by the OIG, the General Accounting Office, and the Department's Office of Independent Oversight and Performance Assurance 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 appropriate officials on September 15, 2003.

PRIOR REPORTS

- *Special Report on Management Challenges at the Department of Energy* (DOE/IG-0580, December 2002). Information technology management remains one of the most serious challenges facing the Department. Although progress had been made in establishing management processes to control information technology planning and investment, and cyber security, the Department must still effectively implement these processes to, among other things, avoid system duplication and minimize vulnerabilities.

- *The Department's Unclassified Cyber Security Program 2002* (DOE/IG-0567, September 2002). The Department had not sufficiently strengthened its cyber security policy and guidance, implemented a cyber security performance measurement system, or established an effective self-assessment program. As a result, critical systems were at risk of unauthorized or malicious use. Furthermore, the potential existed for compromise of sensitive operational and personnel-related data.

- *Cyber-Related Critical Infrastructure Identification and Protection Measures* (DOE/IG-0545, March 2002). While the Department had initiated certain actions designed to enhance cyber security, it had not made sufficient progress in identifying and developing protective measures for critical infrastructures or assets. For example, the audit disclosed that the identification of national priority assets had not been finalized and the specific identification of critical cyber-related assets had not begun. Corrective actions to address issues disclosed by our previous audit of the Department's infrastructure protection program were progressing slowly and remained incomplete. For instance, specific, quantifiable infrastructure protection-related performance measures had not been developed and the Department's critical infrastructure protection plan had not been updated.

- *Virus Protection Strategies and Cyber Security Incident Reporting* (DOE/IG-0500, April 2001). The Department's virus protection strategies and cyber security incident reporting methods did not adequately protect systems from damage by viruses and did not provide sufficient information needed to manage its network intrusion threat. These problems existed because the Department had not developed and implemented an effective enterprise-wide strategy for virus protection and cyber security incident reporting.

- *Implementation of Presidential Decision Directive 63, Critical Infrastructure Protection* (DOE/IG-0483, September 2000). While external energy sector infrastructure protection activities were progressing and a number of internal and collateral actions had been completed, the Department had not implemented its critical infrastructure protection plan to mitigate significant vulnerabilities, or assure the continuity and viability of its critical infrastructures.

- *Unclassified Computer Network Security at Selected Field Sites* (DOE/IG-0459, February 2000). Departmental sites audited had significant internal or external weaknesses that increased the risk that their unclassified computer networks could be damaged by malicious attack. Each site evaluated had network vulnerabilities involving poor password management, unnecessary access to certain powerful computer services, weak configuration management, outdated software with known security problems, and/or problems with firewall configuration.

- *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 2000). GAO noted that a major contributing factor to the existence of the Department's security vulnerabilities was ineffective and inconsistent information technology security management throughout the Department. GAO found that, among other things, the Department had not prepared federally required security plans, effectively identified and assessed information security risks, or fully and consistently reported security incidents.

- *Information Security: Software Change Controls at the Department of Energy* (GAO/ AIMD-00-189R, June 2000). GAO reviewed software change controls at the Department focusing on, among other things, whether key controls as described in agency policies and procedures regarding software change authorization, testing, and approval complied with Federal guidance. They reported that Departmentwide guidance and formal procedures were inadequate and several components reviewed had no formally documented process for routine software change control.

- *Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research* (GAO/ AIMD-00-140, June 2000). Unclassified scientific research information systems were not consistently protected at all Department laboratories. Although some laboratories were taking significant steps to strengthen access controls, many systems remained vulnerable. A major contributing factor to the continuing security shortfalls at these laboratories was that the Department lacked an effective program for consistently managing information technology security throughout the agency.

- *Independent Oversight Safeguards & Security and Cyber Security Inspection of the Los Alamos Site Office and Los Alamos National Laboratory* (December 2002).

- *Independent Oversight Inspection of Cyber Security at the Chicago Operations Office and Argonne National Laboratory* (October 2002).

- *Independent Oversight Cyber Security Inspection of Albuquerque Operations Office* (October 2002).

IG Report No.:DOE/IG-0620

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 audit 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 this 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?

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.