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

Evaluation Report

The Department's Unclassified Cyber Security Program—2005

DOE/IG-0700

September 2005

Department of Energy
Washington, DC 20585
September 27, 2005

MEMORANDUM FOR THE SECRETARY

FROM: Greg Friedman
Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department's Unclassified Cyber Security Program - 2005"

BACKGROUND

The Department of Energy deploys numerous networks and individual information systems to help meet its strategic goals in the areas of national defense, energy, science, and the environment. As with other Federal agencies, the threat of intrusion or damage to these networks and systems continues to grow as cyber related attacks become more sophisticated. The risk to systems and actual damage has been well demonstrated by a series of high profile intrusions and compromises of a number of commercial and Federal systems during the past year. These events reinforce the need for a strong defense to ensure that the Department's mission critical systems, and the important data they contain, remain available to address mission needs. Overall, the Department invests a significant portion of its budget, about $2.7 billion in Fiscal Year 2005, to develop, maintain, and ensure the confidentiality, integrity, and availability of its various systems and networks.

The Federal Information Security Management Act (FISMA), enacted in 2002, was designed to encourage agencies to develop and maintain cyber security controls sufficient to protect information resources. To satisfy evaluation requirements of FISMA, the Office of Inspector General conducts an annual independent evaluation to determine whether the Department's unclassified cyber security program adequately protects data and information systems. This memorandum presents the results of our evaluation for Fiscal Year 2005.

RESULTS OF EVALUATION

To their credit, senior-level management officials have continued to focus their attention on strengthening the Department's cyber security posture. While these actions offer promise, we continued to observe systemic problems that expose the Department's critical systems to an increased risk of compromise. We found that:

- Many required system certifications and accreditations had not been performed, lacked essential elements such as independent testing of the effectiveness of security controls, or were not adequately documented;

- Although critical to planning and implementing protective efforts and in spite of several years of effort, an inventory of information systems had yet to be completed;

- Contingency planning, necessary to ensure that systems could continue or resume operations in the event of an emergency or disaster, had not been completed for certain critical systems;

- Cyber security incidents were not always reported to law enforcement officials as required by Departmental guidance; and,

- Problems with segregation of duties, excessive or inappropriate authority to access or modify information resources, and change control management continued.

These problems occurred, at least in part, because program and field elements did not always implement or properly execute standing Departmental and Federal cyber security requirements. We also noted that the Department had not always taken advantage of lessons learned through independent reviews to strengthen its cyber security posture. As a consequence, the Department's information systems and networks, and the data they contain, remain at risk of compromise. An aggressive, proactive cyber security program that includes the full cooperation and participation of all program and field elements is necessary to help ensure adequate protection of the Department's valuable information technology assets.

In recognition of its many cyber security challenges, Department management had issued several policy memoranda designed to address security weaknesses in areas such as certification and accreditation and the implementation of minimum security configurations. Also, the Department recently initiated a Cyber Security Improvement Initiative. This is a collaborative effort between the Office of Chief Information Officer, the Office of Independent Oversight and Performance Assurance, and the various program offices to conduct joint site visits to identify and resolve cyber security problems, provide site assistance, and follow-up on corrective actions. These are positive steps which, if faithfully implemented, have the potential to significantly improve cyber security across the complex. This report includes several recommendations designed to assist in this process.

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

MANAGEMENT REACTION

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

Attachment

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

EVALUATION REPORT ON THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM – 2005

TABLE OF CONTENTS

Cyber Security Program

Appendices

Program Improvements

We found that the Department of Energy (Department) continued to take steps to strengthen its cyber security program and had implemented a number of countermeasures to reduce network vulnerabilities addressed in our *Evaluation Report on the Department's Unclassified Cyber Security Program-2004* (DOE/IG-0662, September 2004). During the past year, senior-level management officials have focused their attention on protecting the Department's systems and data. In particular, we observed that:

- Several important cyber security policy memoranda addressing security improvements, certification and accreditation, and minimum security configuration requirements had been issued;

- Improvements had been made in the accuracy of the Plan of Action and Milestones (POA&M) database used to report and track cyber security weaknesses; and,

- The overall volume of cyber security findings issued during our evaluation declined from 32 in 2004 to 21 in 2005.

Risk Management

While the Department has made incremental progress in strengthening its cyber security program, additional work is needed to ensure that all components necessary to sustain a comprehensive risk management program are completed. Our evaluation disclosed that despite substantial effort, certification and accreditation and a comprehensive inventory of major systems remain incomplete. At certain sites, organizations had not developed and/or tested system contingency plans. In a number of instances, sites failed to report computer intrusions or other cyber security incidents to law enforcement officials as required. These processes are essential components of a risk management strategy and provide a framework for managing threats to agency operations, assets, and employees resulting from the operation of information systems.

Certification and Accreditation

Certain sites had not completed certification and accreditation (C&A) of all major and general support systems as required by Federal regulation. C&A of information systems enables program officials or system owners to, among other things, develop policies and procedures to address high-risk issues through cost-effective mitigation strategies. Based on an independent review of C&A documentation packages completed by the Office of Chief Information Officer (OCIO) during 2004 and 2005, many of the C&As completed at Headquarters and various sites lacked critical components or had been inadequately documented. Specifically, the OCIO's review of C&A packages for 45 systems disclosed that 39 were inadequate. Various problems were identified including missing POA&Ms, risk assessments, security plans, and/or a lack of accreditation documentation.

Our own tests, and those completed by the Office of Independent Oversight and Performance Assurance (OA), identified additional problems at a number of other sites. At seven of the sites reviewed, we noted problems similar to those identified by the OCIO. For example, organizations failed to conform their C&A actions to National Institute of Standards and Technology (NIST) requirements and omitted or did not adequately document various components including those related to security controls. Certain sites also incorrectly used a broad grouping or "enclave" approach to completing C&A of their systems. In using such an approach, organizations grouped systems together without regard to the security levels of the individual systems within those enclaves. As a consequence, systems rated as high risk were grouped with low risk systems and may not have received adequate protective measures.

Systems Inventory

Even though required by the Federal Information Security Management Act (FISMA), the Department had not yet established a complete inventory of systems. Generally, agencies are required to develop a system inventory that includes an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency. As we reported in our *Evaluation Report on the Department's Unclassified Cyber Security Program* (DOE/IG-0519, August 2001), the Department had started to identify, prioritize, and protect its critical assets during 2001. As of the date of our evaluation, however, the Department had not established a firm methodology or system definition and the effort remained incomplete. As a consequence, reporting varied significantly among sites. In some instances, sites inappropriately grouped a number of systems, some with differing risk levels, and reported that grouping as a single system or enclave. Inventory data gathered by some sites also lacked information regarding how systems were interconnected – data essential for planning and determining necessary protective measures.

Contingency Planning

Five of the 34 sites included in our review 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, four sites had not developed or tested contingency or disaster recovery plans for their financial or other major systems. Additionally, one of the sites had not completed a risk assessment or a continuity of operations plan for its computer center. We also noted that the backup server for a system was located in the same location as its primary production server, thus negating the benefit of the backup server should a localized disaster occur. Our *Audit Report on Management Controls Over Selected Departmental Critical Monitoring and Control Systems* (OAS-M-05-06, June 2005) similarly found that five of the six critical systems we reviewed did not have necessary controls to mitigate foreseeable risks – including the formulation of comprehensive contingency plans, establishment of secondary systems, and adequate protection measures for backup information.

Incident Reporting

Although program elements have improved their reporting of cyber security incidents to the Department's Computer Incident Advisory Capability, we found that incidents were still not always reported to law enforcement officials. As required by FISMA and Department policy, the Office of Inspector General (OIG), Office of Investigations is to be notified of all cyber security incidents that fall into six categories, including compromise/intrusion, web site defacement, malicious code, denial of service, critical infrastructure protection, and unauthorized use. At the time of our evaluation, however, the Department had notified the Office of Investigations of only about half (60 of 108) of the qualifying cyber security incidents that occurred in Fiscal Year (FY) 2005. Failure to report these occurrences jeopardizes the ability to promptly investigate potential criminal cyber security incidents.

Security Controls

Despite significant efforts over the past several years, the Department continued to experience problems in the areas of access controls, segregation of duties, and configuration management. While progress had been made in correcting security control weaknesses identified in previous evaluation reports, we continued to identify problems at over half of the 34 sites included in our evaluation.

Access Controls

The Department continues to experience access control weaknesses across the complex. Even though sites corrected most problems reported last year, we identified 4 repeat and 16 new weaknesses during this year's evaluation. Strong and functional access controls are essential for ensuring that only authorized individuals can access information resources. Access controls consist of both physical and logical controls designed to protect computer resources from unauthorized modification, loss, or disclosure. Access control problems included:

- Seven sites had easily guessed, blank, or vendor default passwords. Since vendor default passwords are widely known, malicious individuals could exploit them to gain access to sensitive information;

- Four sites had passwords that did not comply with Departmental policy. For example, passwords established for a classified network on which a financial system resides, and an unclassified network including support applications, were not sufficiently strong in that they did not contain required special characters;

- Five sites granted system administrators excessive privileges that were not required to perform their assigned duties. These privileges, if exploited, could permit unauthorized or malicious modifications to systems or information; and,

- One site used a group account that permitted database administrators to access production systems. This procedure does not provide an audit trail and could enable unauthorized or malicious modification to data.

Segregation of Duties

Our review disclosed five 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 inadequate segregation of duties regarding application developers with access to production systems that could permit them to introduce untested, unapproved, or malicious changes into active systems. Other users had been granted system privileges that allowed incompatible duties. For example, members of an accounts payable department were granted system privileges that allowed access to the general ledger user module, while other individuals had the assigned duty to both record and delete fixed assets, as well as reconcile the general ledger amounts to sub-ledgers.

Configuration Management and Change Control

Testing at sites covered by our evaluation also revealed 16 instances of configuration management and change control weaknesses. These controls help ensure that computer applications and systems are controlled and protected against unauthorized modifications and are essential to a coordinated and strong security policy. While the Department corrected several problems reported last year, we found similar problems this year at different sites, including:

- Weak patch management, a practice that exposes systems to an increased risk of attack or compromise because available security updates are not applied or are not executed in a timely manner;

- Not replacing or updating software with known vulnerabilities; and,
- Not ensuring that changes to systems or applications were properly managed and controlled.

Cyber Security Program Management

These problems occurred, at least in part, because program elements did not always ensure that Departmental and Federal cyber security requirements were properly implemented. Although required by Office of Management and Budget (OMB) guidance, we noted that the Department had not taken advantage of lessons learned through audits, evaluations, and reviews to strengthen its cyber security posture.

Program Management

Departmental program offices did not always ensure that Federal cyber security requirements, Department policies, and controls were properly implemented by field organizations and facility contractors. In certain cases, as with the C&A process, we noted that program offices set forth implementing procedures that were overly permissive and did not comply with NIST requirements. In other examples, we found that despite Departmental guidance to the contrary, program officials had not ensured that facility operating contracts were modified to incorporate all Federal cyber security requirements.

For example, we learned that a major program office's policy implementing guidance did not specifically require that contractors comply with FISMA, OMB, and NIST cyber security requirements. One contractor-managed field operation did not agree that it was required to comply with such requirements. The contractor-managed field operation of another major program office stated that, even though it agreed it was required to comply with FISMA, OMB, and NIST requirements, it would not comply until the requirement was added to its contract as required by Departmental policy. Failure to comply with these cyber security requirements is critical since the vast majority of the Department's sites are managed and operated by contractors and contract employees comprise over 85 percent of the Department's workforce.

POA&M

Although improvements had been made in the accuracy of the POA&M database, the Department had not used this important management tool to its maximum advantage. While the database has been successfully used as a means to track the status of cyber security weaknesses, its value as a learning tool has been limited because the Department has not disseminated information regarding common findings to its various program elements. Since program and site officials can only access data specifically related to their organizations, they are unable to determine whether weaknesses reported for other organizations may be applicable to their sites. As noted in our report *The Department's Audit Resolution Process* (DOE/IG-0639, February 2004), such evaluations are required by OMB Circular A-50 and could permit organizations to take advantage of lessons learned through audits, evaluations, and reviews to strengthen their cyber security posture. Such actions are particularly relevant within the Department because over the past several years we have noted that, while previous year weaknesses are being corrected, many of the same or similar weaknesses were repeated at other sites in subsequent years.

Resources and Data Remain at Risk

Although the Department continues to make improvements in its unclassified cyber security program, its information systems and networks and the data they contain remain at risk of being compromised. These resources will remain at risk until the Department takes action to proactively manage its cyber security program and ensure implementation of adequate cyber security controls by all program elements, including contractors. Cyber security incidents are on the rise and attempts to probe and penetrate cyber security defenses are becoming increasingly sophisticated. At the time of our review, the Department had been subject to 108 significant cyber security incidents, consisting primarily of worms, unauthorized users, and malicious codes during FY 2005. Inadequate protective measures leave valuable information technology resources vulnerable to cyber attacks from internal and external sources and could result in data tampering, disruption of critical operations, and inappropriate disclosure of sensitive information.

RECOMMENDATIONS

This report identifies weaknesses that should be addressed by the program offices in coordination with the OCIO. Specifically, we recommend that the Administrator, National Nuclear Security Administration, and the Under Secretary for Energy, Science, and Environment, in coordination with the Chief Information Officer (CIO):

1. Correct, through the implementation of management, operational, and technical controls, each of the specific vulnerabilities identified in this report;

2. Take action to analyze and disseminate information on common or recurring cyber security weakness to cognizant program and site officials;

3. Revise program office implementing guidance and contracts to specifically require that site and facility management contractors comply with FISMA, OMB, and NIST cyber security requirements; and,

4. Require program offices to establish a mechanism to ensure that Federal and Departmental cyber security policy and guidance are communicated, understood, and implemented by line management across the complex, including contractors.

MANAGEMENT REACTION

Management generally concurred with our findings and recommendations. Based upon an agreed-upon protocol, management provided informal comments to our report. Such comments were discussed with the OCIO on September 16, 2005, 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 2005 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. OA performed a separate review of classified and national security 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;

- 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 and systems 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 OIG contract auditor. OIG and 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 cyber security review work performed by the OIG, KPMG, the Department's OA, the Government Accountability Office (GAO), and internal Departmental studies.

We also evaluated the Department'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 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 16, 2005.

PRIOR REPORTS

Office of Inspector General Reports

- *Audit Report on Management Controls Over Selected Departmental Critical Monitoring and Control Systems* (OAS-M-05-06, June 2005). The report indicated that the Department could not ensure that selected critical monitoring and control systems could continue or resume operation with minimal disruption and information loss in the event of an emergency. Specifically, management did not always assess risks or take adequate steps to mitigate foreseeable risks. Among other things, the report noted that necessary steps to mitigate foreseeable risks – including the formulation of comprehensive contingency plans, establishment of secondary systems, and adequate protection measures for backup information – had not been completed for five of the systems reviewed.

- *Development and Implementation of the Department's Enterprise Architecture* (DOE/IG-0686, April 2005). The Department had not fully defined its current or future information technology requirements, essential elements if the architecture is to be an effective tool in managing information technology investments. Among other things, the report noted that although the Department had established a repository that would include a complete inventory of existing systems, at the time of the review, the Department had not fully populated the repository with inventory and requirements data.

- *Special Report on Management Challenges at the Department of Energy* (DOE/IG-0667, November 2004). The report stated that the Department continues to improve its information technology management by developing corrective actions to mitigate cyber security risks and to improve relevant controls. For instance, the Deputy Secretary initiated a campaign to complete certification and accreditation of all major applications and general support systems. The OCIO has issued a series of new cyber security policies that address previously reported weaknesses and emphasize a risk-based approach to managing security, that, when implemented, should strengthen cyber security across the Department. The OCIO is also making plans to independently verify and validate the vulnerability reduction steps being taken.

- *Evaluation Report on the Department's Unclassified Cyber Security Program-2004* (DOE/IG-0662, September 2004). Even though the Department's overall cyber security posture has improved, problems continue to exist in the Department's unclassified cyber security program that, if uncorrected could expose critical systems to compromise. The report found that the Department had not completed implementation of a comprehensive risk management program. For example, the Department had not: 1) completed certification and accreditation of each major system to identify and mitigate risks; 2) prepared contingency plans to ensure that mission critical systems could continue in the event of an emergency or disaster; and , 3) ensured adequate security controls were in place at all of the sites.

- *The Department's Audit Resolution Process* (DOE/IG-0639, February 2004). The Department did not fully realize the potential benefit of recommendations addressing internal control weaknesses because, in part, it did not perform trend analyses to identify systemic problems or routinely review audit findings for applicability to others. Despite recommendations in our previous report and requirements of OMB Circular A-50, the Department did not conduct periodic analyses of audit recommendations to identify trends, system-wide problems, and potential solutions. Accordingly, it did not take advantage of the opportunity to determine whether similar issues exist at other programs, activities, or sites.

- *Evaluation Report on the Department's Unclassified Cyber Security Program* (DOE/IG-0519, August 2001). Among other things, the report stated that the Department had not identified all critical information technology assets, an essential step in implementing an effective risk-based, cyber security program. As noted in a recent report, the Department had not developed an information systems baseline that included an inventory of applications and major systems in use or under development. Although the Department has started a process in 2001 to identify, prioritize, and protect its critical assets, the effort remained incomplete.

Government Accountability Office Reports

- *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: Governmentwide 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: the CIO position had been vacant; omissions of requirements from guidance were due to oversights; or the process was being revised.

Office of Independent Oversight and Performance Assurance Reports

- *Independent Oversight Cyber Security Inspection of the Bonneville Power Administration* (November 2004).

- *Independent Oversight Cyber Security Inspection of the Brookhaven National Laboratory* (February 2005).

- *Independent Oversight Cyber Security Inspection of the Southeastern Power Administration* (April 2005).

- *Independent Oversight Cyber Security Inspection of the Southwestern Power Administration* (October 2004).

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

- *Independent Oversight Cyber Security Inspection of the Western Area Power Administration* (April 2005).

IG Report No. DOE/IG-0700

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 Leon Hutton at (202) 586-5798.