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

Evaluation Report

The Department's Unclassified Cyber Security Program—2006

DOE/IG-0738

September 2006

November 2006

Department of Energy
Washington, DC 20585

September 18, 2006

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department's Unclassified Cyber Security Program - 2006"

BACKGROUND

To help accomplish its strategic goals in the areas of defense, energy, science and the environment, the Department utilizes numerous interconnected computer networks and individual systems. Virtually all of the Department's systems are increasingly subjected to sophisticated attacks designed to circumvent security measures, trick unsuspecting users into divulging sensitive information or propagate harmful programs. A strong cyber security program is essential to minimizing adverse impacts to Department mission associated with successful attacks or intrusions and protecting operational, personally identifiable and other sensitive data from compromise. Overall, the Department expects to invest over $295 million in Fiscal Year (FY) 2006 to protect its annual $2 billion investment in information technology resources.

The Federal Information Security Management Act (FISMA) provides a comprehensive framework for ensuring the effectiveness of security controls over information resources that support Federal operations and assets. 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 protects data and information systems. This memorandum presents the results of our evaluation for FY 2006.

RESULTS OF EVALUATION

The Department had taken a number of steps to strengthen its cyber security posture. During the last year, it had launched a cyber security revitalization program and issued enhanced guidance designed to strengthen protective efforts. While these were positive steps, we continued to observe deficiencies that exposed its critical systems to an increased risk of compromise. In several respects, these findings paralleled those reported in 2005. Specifically, for 2006, we found that:

- In spite of recent improvements in reporting methodologies and standards, the Department had not yet completed a complete, site-wide inventory of its information systems;

- Many system certifications and accreditations had not been performed or were inadequate in that they lacked essential elements such as annual self-assessments and independent testing of security controls;

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

- Weaknesses existed in physical, logical access, and change controls designed to protect computer resources from unauthorized modification, loss, or disclosure of information.

Continuing cyber security weaknesses occurred, at least in part, because program and field elements did not always implement properly or execute existing Departmental and Federal cyber security requirements. In a number of instances, cyber security weaknesses exposed through internal and external reviews were not addressed in a timely manner or tracked to resolution. As a consequence, the Department's information systems and networks and the data they contain remain at risk of compromise.

To help address continuing weaknesses, the Department recently launched a revitalization effort designed to improve the management of its cyber security program and to emphasize line management's responsibility – through each of the Under Secretaries – to ensure that systems and data under their operational control are secure. As part of this effort, the Department issued new and updated cyber security guidance designed to strengthen controls over the certification and accreditation process, password management, and the use and control of wireless devices. In addition, the Office of Science's Office of Information Technology Management, in conjunction with the Office of Health, Safety and Security's Office of Independent Oversight, conducted a number of site visits to help identify and quickly resolve cyber security problems. These processes, if implemented complex-wide, should help the Department resolve existing weaknesses and strengthen its overall cyber security posture. To aid the Department in its ongoing efforts, we have made several recommendations designed to enhance overall controls.

The Department and its program elements also recently developed policies and guidance to address Office of Management and Budget requirements for ensuring security over personally identifiable information. We are in the process of conducting a comprehensive review of efforts. Because of its importance to the cyber security program, we are also in the process of conducting a separate review that more fully examines the state of certification and accreditation across the Department.

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

MANAGEMENT REACTION

Management 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
Under Secretary for Science
Chief of Staff
Chief Information Officer

TABLE OF CONTENTS

PROGRAM IMPROVEMENTS

The Department of Energy (Department) continued efforts to strengthen its cyber security program and had implemented a number of measures to reduce vulnerabilities such as those described in our *Evaluation Report on the Department's Unclassified Cyber Security Program – 2005* (DOE/IG-0700, September 2005). Since last evaluation, the Department appointed a new Chief Information Officer who has taken steps to restructure the Department's approach to cyber security. For instance, the *Revitalization of the Department of Energy's Cyber Security Program* was developed to improve the management of the program and emphasized line management's responsibility – through each of the Under Secretaries – to ensure that systems and data under their operational control are secure. Specific components of the revitalization effort include:

- Issuing new and updated cyber security guidance addressing areas such as certification and accreditation, risk management, vulnerability management, contingency planning, password management, wireless devices, and protection of personally identifiable information;

- Initiating a collaborative effort between the Office of Chief Information Officer (OCIO), the Office of Health, Safety and Security's Office of Independent Oversight, and the Office of Science to conduct joint site visits to identify and resolve cyber security problems; and,

- Improving the process for reporting cyber security incidents to law enforcement officials.

In addition, the Department continues to strengthen its defense in depth approach to network protection, a practice that has helped it repel external attacks and reduce the risk of propagation of malicious code, viruses or worms across systems. These efforts, if implemented completely, should help the Department resolve existing weaknesses and strengthen its overall cyber security posture.

MANAGING CYBER RELATED RISK

Inventory and Evaluation of Critical Information Systems

While the Department's revitalization efforts hold promise to improve its overall cyber security posture, existing problems continue to place critical information systems and data at risk of compromise. Our evaluation disclosed that a

comprehensive inventory of all operational information technology (IT) systems, an essential component of a risk-based approach to cyber security, remained incomplete. Certification and accreditation (C&A) of all operational information systems had either not been completed or were inadequate. Most significantly, our testing disclosed that for a number of systems, risk levels and needed control measures had not been properly assessed, implemented, and tested. At certain sites, organizations had not taken appropriate measures to safeguard their systems in the event of an emergency. These processes are essential components of a risk management strategy and provide a framework for managing threats to agency operations, assets, and employees.

Systems Inventory

Even though required by the Federal Information Security Management Act (FISMA), the Department had not yet established a complete inventory of systems. 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. Complete inventory data is essential to determining the risks associated with system operation and interconnection with internal or external resources. The Department had developed a reporting methodology and standard to establish a Department-wide inventory, however, a complete inventory of information systems had not been established. While most sites maintained inventory information, its usefulness was sometimes limited because of issues such as inconsistent approaches to grouping systems and a lack of interconnection information. Completion of a complete, wide inventory is planned for September 2007.

Certification and Accreditation

The Department had not completed or had not adequately performed certification and accreditation of all operational IT systems in accordance with Federal regulation. Specifically, at four sites we identified seven systems, some of which were core operational systems, for which the C&A process had not been completed. At 12 sites, organizations provided us with documentation supporting completion of the C&A process for systems we selected for review; however, we noted that many specific, detailed activities required by guidance

promulgated by the Department and the National Institute of Standards and Technology (NIST) had not been performed. Based on our testing and that performed by the Office of Independent Oversight, we noted that:

- Risk categorization assessments of information systems had not been performed or were inadequate at six sites;

- Certain sites incorrectly used a broad grouping or "enclave" approach to complete C&A of their systems and grouped low risk systems with those requiring higher protection levels;

- At five sites, accreditation boundary information - data necessary to identify all system components - lacked sufficient detail to understand the system and determine the scope of certification and accreditation;

- Security plans at six sites were incomplete or missing critical elements, such as mandatory security controls;

- Independent assessments and certification of the effectiveness of security controls were not completed or documented at four sites as required;

- Annual self-assessments of all systems were not performed or were not performed in accordance with NIST guidance at six sites; and,

- At two sites, the role of Designated Accrediting Authority, the individual responsible for accepting risks associated with system operation and granting authority to operate, had been improperly delegated to a contractor official.

Because of its importance to the Department's cyber security program, the Office of Inspector General is currently conducting a separate audit that more fully examines the state of certification and accreditation across the Department.

Contingency Planning

Although previously reported weaknesses in contingency planning had been corrected, we continued to identify sites that 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, six sites had not

adequately developed or tested contingency or disaster recovery plans for their financial or other major systems. In addition, two sites had inadequate provisions for restoring and backing up systems or system components. Recent events such as the damage associated with Hurricanes Katrina and Rita demonstrate the importance of maintaining robust contingency capability. Inadequate contingency planning could delay restoring critical operations or potentially lead to the loss of critical information should unforeseen and unplanned events such as those occur.

Security Controls

While the Department has taken action to strengthen controls and correct previously reported deficiencies, it continues to experience problems in the areas of access controls, segregation of duties, and configuration management. These controls, generally recognized as establishing a baseline for many other security controls, are essential for protecting systems from unauthorized or malicious modifications to systems or information.

Access Controls

Even though sites corrected most of the access control problems reported last year, testing identified weaknesses at four sites during this year's evaluation. Strong and functional controls of this type are essential for ensuring that only authorized individuals gain access to network or system resources. Controls in this area consist of both physical and logical measures designed to protect computer resources from unauthorized modification, loss, or disclosure. In particular, we noted several instances where sites did not comply with Departmental policy:

- Two sites had blank, easily guessed, and/or original vendor default passwords, thus exposing them to the risk of unauthorized access to databases and operating servers;

- Three sites had passwords that were not changed at set intervals or were not sufficient in strength; and,

- At another site, incorrect login attempts were not restricted, an important control designed to prevent "brute force" access through repeated password guessing.

One site also had not performed sufficient access reviews for the users of its general support system. These reviews are essential to determine whether users who no longer have a valid need to access information systems, such as through job changes or resignations, are denied access to these systems.

Configuration Management and Change Controls

Configuration management and change control issues continue to be a problem and our evaluation identified weaknesses at seven of the Department's sites. Controls of this type help ensure that computer applications and systems are managed to prevent and protect against unauthorized modifications and are essential to a coordinated and strong security policy. We noted problems such as not:

- Replacing or updating software with known vulnerabilities - a process generally known as patch management. Unless properly completed, systems are exposed to an increased risk of attack or compromise because available security updates are not applied or are not executed in a timely manner.

- Ensuring that changes to systems or applications were properly managed and controlled. Change control is the process that management uses to identify, document and authorize changes to an IT environment. For example, one site's documentation did not demonstrate that software changes had been consistently approved by authorized personnel prior to being implemented. A system at another site did not have the audit logging function enabled, a feature that permits the actions performed by users with privileged accounts to be monitored. Without proper change controls, individuals may create and put into production improper, unauthorized, or malicious program modifications.

In addition, configuration standards necessary for ensuring uniformity and adequacy in the level of computer security across the complex were not consistent. Although required by Department and Office of Management and Budget (OMB) guidance, we found that four organizations had not adopted minimum security configuration standards. Also, two organizations had not included procedures in their security plans governing how to document and seek approval for necessary deviations from such standards.

CYBER SECURITY PROGRAM MANAGEMENT

As with previous years, the problems cited in our report occurred, at least in part, because the Department's organizations had not always ensured that Department and Federal cyber security requirements were properly implemented. The OCIO also had not completed required independent verification and validation activities necessary to monitor cyber security performance of program elements. Finally, the Department had not ensured that organizations reported and tracked to resolution all cyber security weaknesses in its Plan of Action and Milestones (POA&M) database.

Implementation of Cyber Security Requirements

Departmental organizations did not always ensure that Federal cyber security requirements, Department policies, and controls were adequately implemented and consistent with Federal requirements, most notably by field organizations and facility contractors. For example, at the direction of the Office of Science, many of its field sites inappropriately applied NIST requirements for categorizing system risk levels and applying corresponding security controls, resulting in systems being protected at a lower level than needed. Many sites also either did not complete or adequately document completion of security control testing and evaluations. Similarly, National Nuclear Security Administration (NNSA) site officials continued to indicate that they were required to comply with NNSA cyber security policy, as opposed to meeting NIST requirements. However, our review disclosed that no NNSA site had fully implemented the NNSA cyber security policy. Instead, many NNSA field sites were permitted to follow a less thorough certification and accreditation process that did not include all NIST or NNSA requirements.

In addition to the issues noted above, the Department had not yet completed the process of modifying facility operating contracts to incorporate all Federal cyber security requirements. Although directives and program guidance are generally incorporated in Contractor Requirements Documents and appended to site/facility management contracts, we learned that the Office of Science and the NNSA had not ensured that this process was completed for FISMA, OMB, and NIST cyber security requirements. Including these requirements in operating contracts is critical

to the success of the cyber security program when one considers that virtually all of the Department's major facilities are managed and operated by contractors.

Department Oversight

Our evaluation also disclosed that the OCIO had not regularly performed independent verification and validation (IV&V) activities essential to evaluating the adequacy of cyber security program performance. While we learned that some IV&V work was performed during May 2005 on selected system certifications and accreditations, findings from these efforts were never remediated. Officials from the OCIO explained that they informed responsible program officials of deficiencies identified, but had taken no other action to ensure that the findings were resolved. Although officials indicated that no additional work in that area had been performed, they also told us that they intended to perform a review of a sample of certification and accreditation packages during 2006. However, at the time of our evaluation, management informed us that it was unable to complete the planned reviews because of other pressing concerns.

Lessons Learned

Similar to problems reported for the last several years, the Department had not always shared, identified, and tracked previously identified cyber security weaknesses. Specifically, the Department did not always use the cyber security POA&M management tool to its maximum advantage and had yet to permit program elements to share vulnerability information for lessons learned purposes. While one of the most powerful features of the database is its ability to track the status of cyber security weaknesses to resolution, its value has been limited because not all findings were included in the database and incorrect finding status was maintained. Our evaluation revealed that:

- Four sites did not use a POA&M to track and report security weaknesses that were discovered internally. These sites only tracked or reported security weaknesses identified by external organizations, such as the Office of Inspector General.

- Four of 25 cyber security weaknesses reported during our Fiscal Year (FY) 2005 evaluation were not recorded and

tracked in the database, and as a consequence, were not included in quarterly status reports to OMB.

- One of 8 repeat findings that were re-issued in FY 2006 was marked as completed in the POA&M database even though it had not actually been corrected.

RESOURCES AND DATA REMAIN AT RISK

Even though the Department has made progress in addressing cyber-related problems, the risk that its information systems, networks, and the data they contain may be compromised remains higher than necessary. Without an increase in focus such as that contemplated in the now-in-process cyber security revitalization plan, it is unlikely that the risk will be substantially reduced. As with other Federal agencies and commercial sector organizations, sophisticated attacks and probes have significantly increased the risk that sensitive operational, personally identifiable, and other sensitive information could be accessed or exfiltrated by malicious entities. At the time of our evaluation, the Department had been subjected to 132 significant cyber security incidents, consisting primarily of attempts to compromise information by unauthorized users, malicious code, and worms during FY 2006 -- a 22 percent increase over last year. Inadequate protective measures leave valuable information technology resources vulnerable to cyber attacks from internal and external sources and could result in data tampering and disruption of critical operations.

RECOMMENDATIONS

To correct the weaknesses identified in this report and improve the effectiveness of the Department's cyber security program, we recommend that the Chief Information Officer, in coordination with the Administrator, NNSA, the Under Secretary for Science, and the Under Secretary for Energy:

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

2. Ensure that cyber security guidance developed by the Department and program offices is in direct compliance with NIST guidance.

3. Complete the process of modifying the facility operating contracts to incorporate all Federal cyber security requirements.

4. Perform compliance monitoring activities to ensure the adequacy of cyber security program performance.

5. Ensure that the POA&M management tool is used to its maximum advantage by identifying, tracking to resolution, and sharing cyber security weaknesses across organizational elements.

MANAGEMENT REACTION

The Department agreed with the information contained in the report and concurred with each of the specific recommendations. It added that it would take appropriate follow up action and continue to work to improve its cyber security posture.

AUDITOR COMMENTS

Management's comments are responsive to our recommendations.

Appendix 1

OBJECTIVE

To determine whether the Department of Energy's (Department) Unclassified Cyber Security Program adequately protected data and information systems.

SCOPE

The audit was performed between February 2006 and September 2006 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 performed a separate review of classified and national security information systems.

METHODOLOGY

To accomplish the audit 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 Department 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 Office of Inspector General (OIG) contract auditor. OIG and KPMG work included analysis and testing of general application controls for systems as well as vulnerability and penetration testing of networks; and,

- Evaluated and incorporated the results of the cyber security review work performed by OIG, KPMG, the Department's Office of Independent Oversight, the Government Accountability Office (GAO), and internal Department 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 drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible 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.

Officials from the Office of Chief Information Officer waived the exit conference.

PRIOR REPORTS

Office of Inspector General Reports

- *Inspection Report on Internal Controls for Excessing and Surplusing Unclassified Computers at Los Alamos National Laboratory* (DOE/IG-0734, July 2006). The report disclosed that Los Alamos National Laboratory (LANL) did not comply with internal controls applicable to excessing and surplusing a computer. This problem resulted in the unauthorized release of a computer hard drive containing unclassified documents. The report found that LANL had not, as required, sanitized the hard drive prior to processing the computer as excess/surplus and removed the hard drive prior to transferring the computer for sale to auction.

- *Special Inquiry Report Relating to the Department of Energy's Response to a Compromise of Personnel Data*, July 19, 2006. The report found that the Department of Energy (Department's) handling of the compromise of personnel data was largely dysfunctional and that the operational and procedural breakdowns were caused by questionable managerial judgments, significant confusion by key decision makers as to lines of authority, responsibility and accountability, poor internal communications, including a lack of coordination and a failure to share essential information among key officials, and insufficient follow-up on critically important issues and decisions.

- *Audit Report on Information Technology Support Services at the Department of Energy's Operating Contractors* (DOE/IG-0725, April 2006). The report revealed that the Department lacked an effective means of managing and controlling contractor information technology (IT) support services costs. The Department had not established a comprehensive framework which would provide a corporate-wide approach to providing IT support services that included contractor-managed sites. Contractors were not required to accumulate information on IT costs or furnish it to Federal officials. The report disclosed that a number of contractors did not actively capture or track functional IT support costs, preventing contractor management and Federal officials from maintaining visibility over the component costs of furnished services.

- *Audit on Management of the Department's Desktop Computer Software Enterprise License Agreements* (DOE/IG-0718, January 2006). The report disclosed that the Department had not fully utilized or designed effective systems to manage its inventory of software licenses, or to track the usage of existing licenses. Specifically, the report stated that sites visited were not able to provide accurate information regarding software maintenance and usage due to the lack of effective systems for tracking such information. Unless progress is made in this area, the Department will continue to have difficulty assessing software needs and usage trends, ensuring effective utilization of existing licenses, and ensuring that enough licenses exist to support software installed on desktops.

- *Evaluation Report on the Department's Unclassified Cyber Security Program - 2005* (DOE/IG-0700, September 2005). The report stated that there were continued systemic problems in the Department's cyber security program that exposed the Department's systems to an increased risk of compromise. The report cited weaknesses in the following areas: system inventory, contingency planning, reporting of cyber security incidents, access controls, segregation of duties and configuration management. These problems occurred, at least in part, because program and field elements did not always implement properly execute Department and Federal cyber security requirements. In addition, 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 remain at risk of compromise.

- *Special Report on Management Challenges at the Department of Energy* (DOE/IG-0712, December 2005). The report identified information technology as one of the Department's most significant challenges related to management weaknesses in the Department's control structure. To its credit, senior level Departmental management officials have focused their attention on improving cyber security posture.

Government Accountability Office Reports

- *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, (GAO-05-552, July 2005). The Government Accountability Office (GAO) found pervasive weaknesses in 24 major agencies' information security policies and practices which threatened the integrity, confidentiality, and availability of Federal information and information systems. Access controls were not effectively implemented; software change controls were not always in place; segregation of duties was not consistently implemented; continuity of operations planning was often inadequate; and security programs were not fully implemented at the agencies. GAO stated that these weaknesses existed primarily because agencies had not yet fully implemented strong information security management programs.

- *Information Security: Emerging Cyber Security Issues Threaten Federal Information Systems* (GAO-05-231, May 2005). GAO found that many Federal agencies had not fully addressed the risks of emerging cyber security threats (spam, phishing, and spyware) as part of their required agency-wide information security programs. In addition, GAO found that federal agencies were not consistently reporting incidents of spam, phishing, and spyware to a central federal entity.

- *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks* (GAO-05-383, May 2005). GAO found that Federal agencies had not fully implemented key controls, such as policies, practices, and tools for operating wireless networks securely. The lack of key controls in federal agencies means

that unauthorized or poorly configured wireless networks could be creating new vulnerabilities. The report found significant security weaknesses at six major federal agencies including signal leakage, insecure configurations of wireless equipment, and unauthorized devices.

- *Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk*, (GAO-05-362, April 2005). GAO reported that most of the agencies reviewed did not have policies or provide guidance in key areas for overseeing the information security practices of contractors, to ensure compliance with contract requirements and agency information security policies. For example, GAO noted that agency policies did not describe oversight methods (including control of agency data in an off-site facility); the frequency of reviews or assessments; key management controls to mitigate unauthorized disclosure of information; physical/logical access controls; or the introduction of unauthorized features, including. Without such policies, agencies may not be able to effectively and efficiently assess the security controls of contractor operations or other users with privileged access to federal data and systems. As a result, GAO concluded that agencies are at increased risk of losing control of network connections, experiencing unauthorized use of information and malicious activity that introduces viruses and worms.

Office of Independent Oversight

- *Independent Oversight Cyber Security Inspection of the Pantex Plant and the Pantex Site Office*, May 2006.

- *Independent Oversight Inspection of Cyber Security at the Savannah River Site*, April 2006.

- *Independent Oversight Unannounced Penetration Test (Red Team) of Department of Energy Headquarters*, February 2006.

- *Independent Oversight Unannounced Penetration Test (Red Team) of the National Renewable Energy Laboratory*, January 2006.

- *Independent Oversight Unannounced Penetration Test (Red Team) of the National Nuclear Security Administration Service Center*, November 2005.

- *DOE Cyber Security Project Team Summary Report and Plan of Action*, November 2005.

Department of Energy
Washington, DC 20585
September 15, 2006

MEMORANDUM FOR RICKEY R. HASS
DIRECTOR, OFFICE OF PERFORMANCE AUDITS
OFFICE OF INSPECTOR GENERAL

FROM: THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER

SUBJECT: Draft Evaluation Report on "The Department's Unclassified Cyber Security Program – 2006"

Thank you for the opportunity to comment on this draft report. The Office of the Chief Information Officer (OCIO) appreciates very much the effort that has gone into this comprehensive report. The information in the report will enable OCIO and the program offices to take appropriate follow-up action on specific findings, as well as to continue to work in the most effective way to improve the Department's cyber security posture. We concur with each of the recommendations in the report.

We appreciate the recognition in the report of the ongoing Department-wide cyber security revitalization effort. The Cyber Security Revitalization Plan establishes a governance framework for cyber security management in the Department through a partnership between OCIO and the Under Secretaries and other senior management to provide adequate protection of all DOE information and information systems. Efforts to date implementing the Plan include issuance by OCIO of cyber security guidance on: Management, Operation, and Technical Controls for Information Systems; Certification and Accreditation; Risk Management for Information Systems; Vulnerability Management; Interconnection Agreements; Plans of Actions and Milestones; Contingency Planning; Password Management; Wireless Devices; Risk Management, and Personally Identifiable Information.

Also, during the last year the Cyber Security Executive Steering Committee was established, which guided the development of the Revitalization Plan, and we also established the Cyber Security Working Group, under the Steering Committee, that participates actively in the development of cyber security guidance and in other cyber security activities. We have made significant improvements to our cyber incident handling capability, including initiating continuing action in real time by a Department-wide cyber forensics team that addresses the most serious cyber attacks that we face. We have improved coordination about incidents with other Federal agencies and improved reporting about cyber incidents to the Inspector General and other key Department organizations. We have engaged in a continuing cyber security awareness campaign involving DOE senior management and the entire complex, especially with regard to actions everyone can take to improve our cyber security posture.

IG Report No. DOE/IG-0738

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 Judy Garland-Smith (202) 586-7828.

This page intentionally left blank.

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.energy.gov

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