



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

Evaluation Report

The Department's Unclassified
Cyber Security Program - 2008

DOE/IG-0801

September 2008




Department of Energy

Washington, DC 20585

September 16, 2008

MEMORANDUM FOR THE SECRETARY

FROM:


Gregory H. Friedman
Inspector General

SUBJECT:

INFORMATION: Evaluation Report on "The Department's
Unclassified Cyber Security Program - 2008"

BACKGROUND

The Department of Energy anticipated spending about \$250 million in Fiscal Year (FY) 2008 to implement cyber security measures necessary to protect its information technology resources – systems and data critical to supporting its mission and business lines of energy security, nuclear security, scientific discovery and innovation, environmental responsibility, and management excellence. Security challenges and threats to the Department of Energy's information systems are continually evolving. Adversaries routinely attempt to compromise its information technology assets. As these attacks become increasingly sophisticated, it is critical that the Department's cyber security protective measures keep pace with the growing threat.

The *Federal Information Security Management Act* (FISMA) provides direction to agencies on the management and oversight of information security risks, including design and implementation of controls to protect Federal information and systems. 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 its information systems and data. This memorandum and the attached report present the results of our evaluation for FY 2008.

RESULTS OF EVALUATION

The Department continues to make incremental improvements in its unclassified cyber security program. Our evaluation disclosed that various sites had taken action to address weaknesses previously identified in our FY 2007 evaluation report by strengthening configuration management of networks and systems and by updating local policies and procedures related to laptop computers and incident reporting. Further, the Office of Chief Information Officer, the National Nuclear Security Administration (NNSA), and program elements had recently issued revised policy that provided direction on management, operating, and technical security controls; and, officials had taken action to incorporate Federal cyber security performance requirements into a number of management and operating contracts. While these are positive accomplishments, additional action is required to further enhance the Department's unclassified cyber security program and help reduce risks to its systems and data. For example, our current review identified opportunities for improvements in areas such as certification and



accreditation (C&A) of systems; systems inventory; contingency planning; and, segregation of duties. Weaknesses that merit further attention include the following:

- A number of C&A issues had been addressed, but problems, particularly in the areas of assessing risks and ensuring the adequacy of security controls, had not been completely resolved;
- Site-level inventories were generally comprehensive and various automated inventory tools had been piloted, however, a system for maintaining a centralized, Department-wide inventory of information systems had not been completely deployed;
- Contingency planning had improved, yet some sites had not completed actions necessary to ensure that system operation could be resumed in a timely manner in the event of a major disruption to services;
- Actions to address cyber incident response issues had been initiated but were not yet complete;
- In some instances, risks to systems had not always been fully assessed to provide assurance that personally identifiable information was adequately protected from loss or unauthorized disclosure; and,
- While many previously identified vulnerabilities in access controls, configuration management and separation of duties had been resolved, we found that weaknesses in these areas continued to exist at various sites.

Similar to our observations during past evaluations, these internal control weaknesses existed, at least in part, because not all Department program organizations, including the NNSA, had revised and implemented policies incorporating Federal and Departmental cyber security requirements in a timely manner. Program officials had also not effectively performed management review activities essential for evaluating the adequacy of cyber security performance. In some cases, officials had not ensured that weaknesses discovered during audits and other examinations were recorded and tracked to resolution. As a consequence, the risk of compromise to the Department's information and systems remained higher than necessary.

To assist the continuing efforts to improve, we made several recommendations designed to help strengthen the Department's unclassified cyber security program and thereby protect its computer resources from unauthorized modification, loss, or disclosure of information.

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, and, in many instances, initiated corrective actions.

MANAGEMENT REACTION

Management concurred with our findings and recommendations. Management's comments are included in their entirety in Appendix 3.

Attachment

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

EVALUATION REPORT ON THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM - 2008

TABLE OF CONTENTS

Unclassified Cyber Security Program

Details of Finding	1
Recommendations and Comments.....	9

Appendices

1. Objective, Scope, and Methodology	11
2. Prior Reports.....	13
3. Management Comments	17

Unclassified Cyber Security Program

Program Improvements

The Department of Energy (Department or DOE) continued to make progress in enhancing its unclassified cyber security program and addressing previously identified cyber security weaknesses. For instance:

- Various sites took steps to correct previously identified weaknesses by strengthening system access controls and configuration management, implementing segregation of duties, developing contingency plans, and updating local cyber security policies and procedures;
- Although not fully implemented, the Office of Chief Information Officer (OCIO), the National Nuclear Security Administration (NNSA), and the Office of the Under Secretary had recently issued revised policy that provided direction on management, operating, and technical controls;
- NNSA and program elements incorporated Federal cyber security requirements into a number of management and operating contracts;
- Action had been initiated to eliminate duplicative incident response capabilities; and,
- Finally, a formal working group was established to ensure that Department cyber security guidance complied with National Institute of Standards and Technology (NIST) guidance.

Managing Cyber Related Risk

The Department continued to improve the management of its cyber security program. However, additional action is needed to reduce the risk of compromise to information systems and data. In particular, weaknesses continued to exist in the Department's certification and accreditation (C&A) process, systems inventory, contingency planning, cyber security incident management, and privacy information controls. These processes are essential for ensuring a comprehensive and effective risk management strategy for protecting information technology systems and data.

Certification and Accreditation

System C&A are critical activities that support a risk management process and are an integral part of an

agency's information security program. A strong and comprehensive process is necessary to ensure that agency officials have the most complete, accurate and trustworthy information possible on the security status of their information systems in order to make informed decisions on whether to authorize their operation. However, our evaluation revealed weaknesses in the process at three sites. We also noted that problems identified at four other sites during our Fiscal Year (FY) 2006 evaluation had not yet been completely corrected. Specifically:

- System security plans at five sites were missing essential components such as descriptions of mandatory security controls. This information is necessary for management to determine that all systems risks have been fully considered and mitigating controls are in place, as necessary;
- Required annual self-assessments of mandatory security controls had not been performed at four sites. Such assessments allow management to identify deficiencies in security controls and the extent to which corrective actions are necessary;
- Independent assessments of security controls had not been adequately performed in conjunction with the certification process at four sites. Such assessments help provide assurance of the adequacy of security controls;
- Testing of security controls at one site was not adequate, in that it did not incorporate an evaluation of certain mandatory security controls. Inadequate testing could potentially result in undetected cyber security weaknesses; and,
- Two sites had not yet completed C&A for certain systems, a deficiency first reported in FY 2006.

Systems Inventory

Despite a longstanding need, the Department had not yet established a complex-wide inventory of information systems. Agencies are required to develop an 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.

Per Office of Management and Budget (OMB) guidance, self-reporting of contractor systems or networks used or operated by a contractor on behalf of an agency without agency verification or validation by the agency is not sufficient. If properly implemented, an automated asset management system could assist the Department in not only *Federal Information Security Management Act* (FISMA) reporting, but also in areas such as risk management, capital planning, and configuration management.

To meet FISMA reporting requirements, the Department's current systems inventory process consists of an annual data call to sites and organizations, resulting in inventory information that is received too late to be adequately verified or validated complex-wide. Such information also does not identify interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency. As a substitute for the annual data calls, the Department has initiated an effort to deploy several FISMA reporting tools with capabilities to capture systems inventory information. However, this initiative, begun in FY 2007, had not been completed. While viewed as an incremental step by one Department official, another noted that the tools would not provide the benefits of a fully automated complex-wide asset management system, including actual identification of system connections and timely configuration and patch management capabilities.

Contingency and Disaster Recovery Planning

Although contingency planning processes at several sites improved, we found that other sites had not initiated or completed actions necessary to ensure that critical operations could be recovered or established at a secondary processing location in the event of a major disruption of services. Specifically, our evaluation disclosed problems with contingency plans at three sites. For instance, one site had not adequately developed and tested its contingency plans. Had it done so, this site would most likely have determined that its primary and secondary processing locations were interdependent, as well as in close proximity to each other and therefore subject to the same hazards.

Cyber Incident Management

We noted that individual program and cyber incident response organizations were not required to adhere to a coordinated/common approach for incident reporting. As a consequence, incident reports reaching the Department's Computer Incident Advisory Capability lacked essential elements for reporting to law enforcement and subsequent analysis for trending. Also, in the event of a multi-site cyber attack on the Department's networks and systems, this reporting environment made it difficult for the Department to develop a coordinated response. These issues were highlighted in our report on *The Department's Cyber Security Incident Management Program* (DOE/IG-0787, January 2008). To the Department's credit, when we informed management of these issues, corrective actions were initiated. Specifically, a comprehensive plan is now underway to implement an Enterprise Incident Capability to eliminate duplicative activities and improve incident management. Management had established a target date of December 31, 2008, for eliminating this duplication.

Privacy Information Controls

Although progress had been made, the Department had not fully assessed the risk to personally identifiable information (PII) on its systems and provided assurance that information collected and maintained was adequately protected from loss or unauthorized disclosure. The protection of PII in Federal systems is critical because its loss or disclosure can lead to serious consequences to individuals, such as identity theft. During the evaluation, we observed that the Department had completed, approved, and posted privacy impact assessments for a number of systems that collect and maintain privacy information, in accordance with OMB direction. However, we also noted that, privacy impact assessments of certain systems either had not been performed or were missing key information for providing assurance of adequate protection. Specifically, one Department organization had not completed and submitted privacy impact assessments for approval by the Chief Privacy Officer, despite having systems that collect and maintain such information. Also, approved privacy impact assessments for other Department organizations were missing necessary information. This information should have been supplied at the time of approval, since it was necessary to provide the level of

assurance that risks had been properly assessed and protective measures were adequate. We also noted that content on a number of the Department's publicly accessible web servers was not always controlled and periodically reviewed. These weaknesses contributed to a number of incidents that involved the exposure of PII to unauthorized or malicious sources.

Security Controls

The Department had not resolved certain previously identified weaknesses at several sites in the area of configuration management. We also identified new weaknesses in segregation of duties and access control areas at other sites. Controls such as these are vital for preventing unauthorized access and modification to systems or information. Our testing did confirm that a number of previously reported cyber security control deficiencies had been corrected.

Access Controls

While sites corrected access control problems identified during our previous evaluations, work performed this past year has disclosed new weaknesses at three sites. Access controls consist of both physical and logical measures designed to protect information resources from unauthorized modification, loss, or disclosure. To ensure that only authorized individuals can gain access to networks or systems, controls of this type need to be strong and functional. However, we noted the following:

- At one site, an administrator of a financial system was granted excessive privileges that were not required to perform assigned duties. These excessive privileges, if exploited, could permit unauthorized modification to the system or information. Passwords for this system were also not of sufficient strength;
- At the same site, insufficient reviews were performed of user access to the network. Such reviews are essential to determine whether users who no longer have a valid need for information resources because of job changes or resignations have their access removed in a timely manner;
- Another site allowed excessive login attempts on its network, thereby limiting the ability to prevent

unauthorized access through repeated password guessing; and,

- A third site allowed unsupervised foreign visitors to use their laptops while connecting to the site's Intranet. Such connection could have permitted individuals to probe the site's network for vulnerabilities, implant malicious code, or remove data without authorization.

Segregation of Duties

One site did not maintain adequate segregation of duties on a financial system. Proper segregation of duties reduces the risk of fraudulent activities by separating personnel activities through operating procedures, supervision, and review. Specifically, application developers had access to the production portion of the financial system, which could enable them to introduce untested or unapproved changes to the system. Furthermore, the site had not enacted the compensating control of management review and approval of developer activities.

Configuration Management

We continued to identify configuration management issues in the Department. Controls of this type are an integral component of a strong security policy and help to ensure that computer applications and systems are consistently configured with minimum security standards to prevent and protect against unauthorized modifications. Our evaluation identified weaknesses at a number of the Department's sites. Specifically:

- Two sites were using versions of application and operating system software that were outdated or not appropriately patched. If software with known vulnerabilities is not updated in a timely manner, risk increases that systems could be compromised;
- A number of Department sites or organizations had not disabled unneeded computer services for their publicly accessible websites. These services increased the risk of malicious damage to these websites;

-
- Although the Department had developed and published policy requiring the adoption of standard desktop configurations, including standard security settings, certain organizations and sites had not yet implemented the protective measures;
 - At one site, a financial system was not set to log account administration activity, an essential control which permits management reviews; and,
 - Security controls at another site on most computers assigned to foreign nationals from non-sensitive countries were not implemented. This problem could enable users to modify log-on settings, load unauthorized software, remove installed software, change computer settings, and ultimately permit unauthorized access to the site's information systems.

**Cyber Security
Program Management**

The problems identified occurred, at least in part, because NNSA and certain Department program elements had not revised and implemented policies and guidance incorporating Federal and Departmental cyber security requirements in a timely manner. They also had not effectively performed review and oversight activities essential for evaluating the adequacy of cyber security performance, and had not ensured that Plans of Action & Milestones (POA&M) were used effectively.

Cyber Security Policy Development and Implementation

Department elements did not act in a timely manner to revise and issue policies and guidance to incorporate Federal and Departmental cyber security requirements, thus limiting their use by sites and organizations during FY 2008. For instance, NNSA did not approve its Policy Letters until May 2008, eight months into FY 2008. An NNSA official told us that site implementation could not be expected until sometime in FY 2009. Also, recently issued cyber security incident reporting guidance does not fully address reporting issues and coordination issues facing the various cyber intrusion and analysis organizations and does not specifically require that incidents be reported to law enforcement or counterintelligence officials. Clear policies, with timely implementation, are necessary to ensure that a consistent baseline exists for monitoring performance.

Management Review

As with last year's evaluation, various levels of Department management had not effectively performed review and management activities essential for evaluating the adequacy of cyber security performance, and had not ensured that POA&Ms were always used effectively. For instance, as of August 2008, 33 reviews of C&A packages had been conducted by a compliance team for the OCIO. However, an official indicated that the compliance team had not published or provided feedback to the submitting organizations regarding the reviews. Also, the Office of Science discontinued its site assisted visits process. This process had been established to increase the effectiveness of the security program and to address findings in prior evaluation reports. When asked about a replacement for the process, an official indicated that an agreement would be explored with the Office of Cyber Security Evaluations to assist in performing this function.

Despite concurring with a prior OIG recommendation, NNSA had taken only limited action to establish an oversight process to ensure effective implementation of Federal cyber security requirements by field organizations and facility contractors. An official indicated that NNSA was in the process of changing their site assessment program. While four assessments had been completed by NNSA, no additional ones had been scheduled. We also noted problems in the manner that certain of these assessments were performed. For instance, one assessment cited significant weaknesses that required resolution, but nonetheless granted a passing score.

We also noted ongoing problems regarding the use of POA&Ms as a management tool for tracking all known cyber security weaknesses to resolution. As noted in NIST guidance, POA&Ms are important for managing an entity's progress towards eliminating gaps between required security controls and those that are actually in place. The Department concurred with the recommendations in our Evaluation Report on *The Department's Unclassified Cyber Security Program - 2007* (DOE/IG-0776, September 2007), and indicated that it would ensure that POA&Ms would be utilized as a tool for prioritizing corrective actions and tracking all known cyber security weaknesses to resolution. However, we observed that this action had not been adequately implemented. Specifically, we found that the

POA&Ms did not contain all cyber security weaknesses identified by the Office of Health, Safety and Security, Office of Inspector General, and the Government Accountability Office. Until the POA&Ms capture all identified weaknesses, they will not be an effective tool for reporting, prioritizing, and resolving vulnerabilities such as those identified in this report. Furthermore, we also determined that 27 percent of the weaknesses identified were about one year beyond their projected remediation dates.

**Threats to Information
Technology Assets
And Data**

During FY 2008, the Department took a number of positive and proactive steps designed to improve its cyber security program. As recognized by senior Department officials, such action is necessary to protect systems and the information they contain from increasingly sophisticated and persistent attacks. The importance and need for sustained action is well demonstrated by the increases in reported cyber security incidents across the complex. Despite strong defense-in-depth network protective measures, and with over a month remaining in FY 2008 at the time of our evaluation, sites had reported 480 cyber security incidents affecting 703 machines to the Department's Computer Incident Advisory Capability. This represents an increase of about 45 percent over the prior year and about 136 percent since 2004. In addition, 127 incidents involved PII, an increase of about 165 percent from those reported in FY 2007.

RECOMMENDATIONS

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

1. Correct, through the implementation of management, operational, and technical controls, each of the specific vulnerabilities identified in this report;
2. Ensure that development and implementation of cyber security policies, including Program Cyber Security Plans, are in accordance with appropriate Federal and Departmental requirements;

3. Strengthen the management review process to include:

- Better monitoring of field sites to ensure the adequacy of cyber security program performance, and,
- Utilizing the POA&Ms for capturing and tracking all known cyber security weaknesses to completion.

**MANAGEMENT
REACTION**

The Department and NNSA agreed with the information contained in the report and concurred with each of the specific recommendations. Management added that it would take corrective action on specific findings and continue to work to improve its cyber security posture.

**AUDITOR
COMMENTS**

Management's comments are generally 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 evaluation was performed between February 2008 and September 2008 at numerous 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 evaluation of the Department's Information Security Program for National Security Systems.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and directives pertaining to cyber security and information technology resources such as the *Federal Information Security Management Act*, Office of Management and Budget Circular A-130 (Appendix III), and DOE Order 205.1A Department of Energy Cyber Security Management;
- Reviewed applicable standards and guidance issued by the National Institute of Standards and Technology;
- 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 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 OIG, KPMG, the Department's Office of Independent Oversight, and the Government Accountability Office.

The evaluation was conducted in accordance with generally accepted Government auditing standards for performance audits. Those standards require that we plan and perform the effort to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our objective. Accordingly, we assessed significant internal controls and the Department's implementation of the *Government Performance and Results Act of 1993* and determined that it had established performance measures for unclassified cyber security. Because our evaluation was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our evaluation. We did not rely solely on computer-processed data to satisfy the objective of the evaluation. However, computer-assisted audit tools were used to perform probes of various networks and drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests. In addition, we confirmed the validity of other data, when appropriate, by reviewing supporting source documents.

The Department waived an exit conference.

PRIOR REPORTS

Office of Inspector General Reports

- *Special Report on The Department's Unclassified Foreign Visits and Assignments Program* (DOE/IG-0791, March 2008). The Department of Energy's (Department), Office of Inspector General (OIG) discovered that the National Nuclear Security Administration (NNSA) had not fully mitigated the risk of foreign nationals gaining unauthorized access to its unclassified Intranet. An incident involving cyber security occurred was noted because of this deficiency. Not all computers assigned to foreign nationals and assignees were properly installed with security features that would prevent one from circumventing security measures such as modifying log-on setting, loading unauthorized software, removing software, and changing systems. In addition, some foreign visitors and assignees had unsupervised use of their foreign government, university, or business laptops within laboratory facilities which had live Intranet connections.
- *Audit Report on Management of the Department's Publicly Accessible Websites* (DOE/IG-0789, March 2008). Our audit revealed that some of the Department's publicly accessible websites did not meet Federal accessibility requirements or contingency planning and emergency response best practices. In addition, content on publicly accessible web servers was not always controlled and reviewed periodically. This resulted in an additional eight instances that involved personally identifiable information (PII) being exposed to unauthorized or malicious sources. In addition, the majority of the organizations failed to implement contingency/emergency planning, provide accessibility to those with disabilities, and limit/disable unneeded computer services due to the lack of guidance from Headquarters and deficiencies in site-level management and control.
- *Audit Report on The Department's Cyber Security Incident Management Program* (DOE/IG-0787, January 2008). Our audit found that program elements and facility contractors had established and operated as many as eight independent cyber security intrusion and analysis organizations whose missions and functions were partially duplicative and not well coordinated. Sites could also choose whether to participate in network monitoring activities performed by the organizations. Furthermore, the Department had not adequately addressed related issues through policy changes, even though it had identified and acknowledged weaknesses in its cyber security incident management and response program.
- *Inspection Report on Incident of Security Concern at the Y-12 National Security Complex* (DOE/IG-0785, January 2008). An unclassified laptop computer was brought into Y-12's limited area without proper authorization and it was not detained by cyber security personnel. The written report for this incident was not completed within the 32 two hour reporting requirement under the Department's Incidents of Security Concern Program. The investigation determined that 37 additional laptop computers may have

Appendix 2 (continued)

- been improperly introduced into the Limited Area by Oak Ridge National Laboratory (ORNL) personnel in recent years. These incidents were not properly reported in a timely manner.
- *Special Report on The Management Challenges at the Department of Energy* (DOE/IG-0782, December 2007). Cyber security was identified as one of the management challenge areas due to several DOE OIG reviews which emphasized the need to improve the Department's overall cyber security program. Despite recent efforts and progress, the Department had not completed its complex-wide inventory for the information systems and certification and accreditation (C&A) of many systems was inadequate.
 - *Audit Report on the Continuity of Operations at Bonneville Power Administration* (DOE/IG-0781, November 2007). Bonneville's continuity of operations capability was not fully compliant with Federal Preparedness Circular 65 (FPC 65) for all of its essential functions. Specifically, Bonneville's primary and alternate facilities for power scheduling were interdependent as well as in close proximity, therefore, were subject to the same hazards. In addition, Bonneville's plan to recover transmission scheduling from disruptions to its primary automated system relied in part on a manual process rather than a fully automated system as required by FPC 65.
 - *Evaluation Report on The Department's Unclassified Cyber Security Program - 2007* (DOE/IG-0776, September 2007). Problems persisted with the certification and accreditation of Department's systems related to assessing risks and ensuring the adequacy of security controls. The Department had not established a complex-wide inventory system and a number of organizations still had not ensured their contingency plans are in working order. Additional deficiencies were identified that reduce the Department's ability to protect its computer resources from unauthorized actions, so the Department could not always ensure the personal information on agency systems was adequately protected. Therefore, the risk of compromise to the Department's information and systems remains higher than acceptable.
 - *Audit Report on Security Over Personally Identifiable Information* (DOE/IG-0771, July 2007). The Department had not fully implemented all protective measures recommended by the Office of Management and Budget (OMB) and required by the National Institute of Standards and Technology (NIST). In particular, we observed that sites reviewed had not identified information systems containing personally identifiable information (PII), or fully evaluated the risks of exposing PII stored in such systems; controls for securing remote access to site-level systems containing personal information had not been fully implemented; and sites had not identified mobile computing devices containing PII nor ensured that this information was encrypted as required by OMB. These problems occurred because Headquarters and site-specific policies did not address all OMB and NIST requirements. Even when policies were clear, programs and sites did not always enforce the requirements to ensure that all necessary controls were in place for protecting PII.

Appendix 2 (continued)

- *Audit Report on The National Nuclear Security Administration's Implementation of the Federal Information Security Management Act* (DOE/IG-0758, February 2007). Cyber security weaknesses have been a continuing challenge for NNSA. Specifically, NNSA did not always properly implement its own guidance as well as Departmental and Federal cyber security requirements. In addition, NNSA had not performed regular monitoring activities essential to evaluating the adequacy of cyber security program performance. As a consequence, NNSA's unclassified information systems and networks and the data they contain remain at risk of being compromised, including the possible unlawful diversion of operational data, PII, or other critical information.
- *Inspection Report on Excessing of Computers Used for Unclassified Controlled Information at the Idaho National Laboratory* (DOE/IG-0757, February 2007). Personnel at Idaho National Laboratory (INL) had sold a computer containing unclassified controlled information that included personal information at a public auction in October 2004. When a new company was awarded a contract to manage INL, the Idaho Operations Office delayed incorporating updated Department directives and used existing internal policies and procedures for computer disposal during a 16-month period beginning in November 2004. INL did not have adequate policies and internal controls for excessing computers and other electronic memory devices to prevent the unauthorized dissemination of unclassified controlled information.
- *Audit Report on Certification and Accreditation of Unclassified Information Systems* (DOE/IG-0752, January 2007). Despite recent efforts by the Department to enhance cyber security guidance, many systems were not properly certified and accredited prior to becoming operational. For example, 9 of the 14 sites reviewed did not properly assess security risks to their systems and did not adequately test and evaluate security controls. In many instances, senior agency officials accredited systems although required documentation was inadequate or incomplete, such as incomplete inventories of software and hardware included within defined accreditation boundaries. In addition, the Office of the Chief Information Officer and program elements did not adequately review completed activities for quality or compliance with requirements.
- *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory* (November 2006). Classified documents were found on a flash drive during a search by Los Alamos County Police at the home of a Los Alamos National Laboratory contractor employee. From this inquiry, we found that the security framework at the lab was seriously flawed. Contributing factors were that security policy in a number of key areas was non-existent, applied inconsistently, or not followed. In addition, monitoring by both Laboratory and Federal officials was inadequate; critical security functions were not adequately segregated; and, physical verification of the accuracy of security plans by Federal and Laboratory officials was not performed.

Appendix 2 (continued)

Government Accountability Office Reports

- *Information Security Progress Reported, but Weaknesses at Federal Agencies Persist* (GAO-08-571T, March 2008).
- *Information Security - Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies* (GAO-08-496T, February 2008).
- *Information Security: Protecting Personally Identifiable Information* (GAO-08-343, January 2008).
- *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats* (GAO-07-705, June 2007).
- *Information Security: Persistent Weaknesses Highlight Need for Further Improvement* (GAO-07-751T, April 2007).

Office of Health, Safety and Security Reports

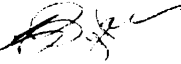
- *Independent Oversight Classified and Unclassified Cyber Security Inspection of the Livermore Site Office and the Lawrence Livermore National Laboratory*, June 2008.
- *Independent Oversight Red Team Activity Report, 2007 Facility Representative Workshop*, March 2008.
- *Office of Independent Oversight Cyber Security Inspection of the Sandia Site Office and the Sandia National Laboratories (U)*, December 2007.
- *Independent Oversight Inspection of Classified and Unclassified Cyber Security at the Nevada Site Office and Nevada Test Site*, December 2007.
- *Independent Oversight Inspection of Cyber Security at the U.S. Department of Energy Headquarters*, October 2007.



Department of Energy

Washington, DC 20585
September 8, 2008

MEMORANDUM FOR RICKEY R. HASS
ASSISTANT INSPECTOR GENERAL FOR
FINANCIAL, TECHNOLOGY, AND CORPORATE
AUDITS

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

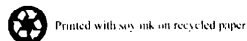
SUBJECT: Draft Evaluation Report on "The Department's
Unclassified Cyber Security Program – 2008"

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 report, including recognition of the additional progress that has been made in the past year, including reduction in the number of identified site-level cyber security weaknesses in the field. 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.

This year, the Department's cyber security team has developed cyber security directives that institutionalize the DOE-wide risk-based approach to cyber security management. These directives build on the cyber security guidance and technical and management requirements (TMRs) documents that we developed earlier. One directive, addressing certification and accreditation and cyber security responsibilities, has been signed. Other directives, addressing minimum controls, incident handling, and media sanitization, are near completion.

We have made significant progress toward streamlining the Department's cyber security incident management process, and expect to complete consolidation of incident handling capabilities this fall. We are also updating our analysis tools and other capabilities for more effective handling of the increasing number of increasingly more sophisticated cyber attacks facing the Department. We believe that the success of the Department-wide cyber security awareness and training programs has improved the detection and reporting of cyber security incidents, enabling DOE to mitigate the effects of those attacks and further improve our overall defense in depth.

We have made progress this year toward implementing tools for tracking corrective actions, performing certification and accreditation, ensuring secure system configurations, and improving system inventory. Progress has been made despite having to redirect some efforts as a result of new OMB direction implementation issues with government-wide Information Security Line of



Appendix 3 (continued)

Business (ISSI oB) tools. As a result, DOE was required to identify alternative solutions to meet the Department's requirements. Some tools are now in use and we are on track through applying good management practices to continue deploying these solutions in FY 2009.

With regard to the specific recommendations in this draft report:

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

Concur. Corrective action plans will be prepared by the programs and by OCIO, as appropriate, as soon as detailed information about specific vulnerabilities is provided.

Recommendation 2: Ensure the timely revision and implementation of policies and guidance by NNSA, Program Offices and field sites to incorporate Federal and Departmental cyber security requirements.

Concur. The programs are already required to take this action by DOE Order 205.1A and the other cyber security directives. OCIO compliance reviews of Program Cyber Security Plans (PSCPs) will continue to focus on this issue. NNSA updated and revised its cyber security policies in April 2008, and the next annual updates are scheduled for Spring 2009. The next round of compliance reviews will be completed by September 2009.

Recommendation 3: Strengthen the management review process to include:

- *Better monitoring of field sites to ensure the adequacy of cyber security program performance*
- *Utilizing the POA&Ms for capturing and tracking all known cyber security weaknesses to completion*

Concur. This is a continuing function of each level of DOE management, including the Under Secretaries through their PSCPs, to ensure that adequate cyber security protections are in place and field program performance is adequate. OCIO will be reviewing POA&Ms in more depth during the coming year as tools are deployed for improved documentation and top-level oversight of the POA&M process. OCIO will continue to review a sample of certification and accreditation packages from across the Department as one indicator of the adequacy of cyber security program performance.

If you need additional information, please contact Bill Huntman, Associate CIO for Cyber Security at (202) 586-4775.

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.