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

Evaluation Report

The Department's Unclassified
Cyber Security Program - 2009

October 2009

Department of Energy
Washington, DC 20585

October 16, 2009

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
                    Inspector General

SUBJECT: <u>INFORMATION</u>: Evaluation Report on "The Department's
                                 Unclassified Cyber Security Program"

<u>BACKGROUND</u>

Industry experts report that security challenges and threats are continually evolving as
malicious activity has become more web-based and attackers are able to rapidly adapt
their attack methods. In addition, the number of data breaches continues to rise. In an
effort to mitigate and address threats and protect valuable information, the Department of
Energy anticipated spending about $275 million in Fiscal Year (FY) 2009 to implement
cyber security measures necessary to protect its information technology resources. These
systems and data are designed to support the Department's mission and business lines of
energy security, nuclear security, scientific discovery and innovation, and environmental
responsibility.

The Federal Information Security Management Act of 2002 (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 2009.

<u>RESULTS OF EVALUATION</u>

The Department continued to make incremental improvements in its unclassified cyber
security program. Our evaluation disclosed that most sites had taken action to address
weaknesses previously indentified in our FY 2008 evaluation report. They improved
certification and accreditation of systems; strengthened configuration management of
networks and systems; performed independent assessments; and, developed and/or
refined certain policies and procedures. In addition, the Department instituted a
centralized incident response organization designed to eliminate duplicative efforts
throughout the Department. As we have noted in previous reports, the Department
continued to maintain strong network perimeter defenses against malicious intruders and
other externals threats.

These are positive accomplishments. However, in our judgment, 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 security planning and testing, systems inventory, access controls, and configuration management. In particular, we issued a number of findings at sites managed by the National Nuclear Security Administration (NNSA). We also identified weaknesses across various Department program elements. Issues that warrant further attention include:

- Weaknesses such as outdated security plans and not completing annual security control self-assessments were identified at several sites;

- The Department had not yet resolved systems inventory issues and had yet to deploy a complex-wide automated asset management tool to help track information technology resources and identify interfaces between systems or networks;

- Although certain improvements had been made to enhance access controls, we noted deficiencies such as a lack of periodic account reviews and inadequate password management at a number of sites; and,

- Previously identified weaknesses in configuration management had been corrected, however, we found problems related to weak administrator account settings and failure to install software patches, as well as incomplete implementation of the Federal Desktop Core Configuration.

These internal control weaknesses existed, at least in part, because certain cyber security roles and responsibilities were not clearly delineated. Program officials also had not effectively performed monitoring and 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 evaluations were recorded and tracked to resolution in the organizations' Plans of Action and Milestones. Our testing disclosed that about 39 percent of existing corrective action milestones had missed estimated remediation dates, with many exceeding planned completion dates by at least one year. 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 the Department's managers to strengthen the 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

EVALUATION REPORT ON THE DEPARTMENT'S UNLCASSIFIED CYBER SECURITY PROGRAM - 2009

TABLE OF CONTENTS

<u>Unclassified Cyber Security Program</u>

<u>Appendices</u>

Program Improvements

The Department of Energy (Department or DOE) continued to make incremental progress over the past year in addressing previously identified cyber security weaknesses and enhancing its unclassified cyber security program. For instance, we noted that actions had been taken to correct seven of nine findings identified during our evaluation of *The Department's Unclassified Cyber Security Program – 2008* (DOE/IG-0801, September 2008). In particular, the Office of Science (Science) and Under Secretary of Energy program elements took action to close all of their findings previously identified by the Office of Inspector General (OIG). In addition, the National Nuclear Security Administration (NNSA) closed four of six findings from last year. Specific actions taken included:

- Improvements in the area of certification and accreditation activities at various sites, including updating security plans to account for current controls and correcting deficiencies identified through control testing;

- Deployment of independent certification agents at sites to perform and validate security control testing results;

- Six sites had updated certain security policies and procedures related to self-assessments, independent assessments, and access controls to correct deficiencies identified during last year's evaluation;

- Correcting configuration management vulnerabilities such as implementing a new process for updating network services and performing regular vulnerability scans; and,

- Instituting a centralized incident response organization that eliminated duplicative efforts throughout the Department.

Managing Cyber Related Risks

As noted above, the Department continued to improve the management of its cyber security program. For example, similar to last year, our evaluation disclosed that the number of overall findings issued to the Department related to risk management had significantly decreased from prior years. In particular, we did not identify any significant issues related to contingency planning or system categorization during our current evaluation. We did, however, determine that additional improvements are possible and should help to further reduce

_____

Details of Finding

the risk of compromise to the agency's information systems and data. In particular, we identified weaknesses in the areas of security planning and testing and maintaining a complete systems inventory. These processes are essential for ensuring a complete and effective risk management strategy for protecting information technology (IT) systems and data.

<u>Security Planning and Testing</u>

Security planning and testing are critical activities that support a risk management process and are an integral part of an agency's information security program. However, as identified in our reports on *Cyber Security Risk Management Practices at the Southeastern, Southwestern, and Western Area Power Administrations* (DOE/IG-0805, November 2008), and *Cyber Security Risk Management Practices at the Bonneville Power Administration* (DOE/IG-0807, December 2008), the Power Marketing Administrations (PMAs) had allowed many security plans to expire or had not developed security plans for all applicable systems. While these same weaknesses were reported in our prior Federal Information Security Management Act (FISMA) evaluation, we noted that a number of the deficiencies had yet to be corrected. A comprehensive system security plan is essential for agency officials to determine that all system risks have been fully considered and necessary mitigating controls are in place.

Additionally, certain PMAs had not always completed annual self-assessments of security controls. For example, one PMA did not perform physical testing of controls but rather relied upon discussion of the controls to determine whether they were properly implemented and operating as intended. In another instance, a PMA mistakenly relied on the Department's Office of Health, Safety and Security (HSS) to satisfy the certification requirements for all systems even though HSS did not test all applicable National Institute of Standards and Technology (NIST) controls and its inspections were not meant to be a substitute for certification testing.

<u>Systems Inventory</u>

Although identified as a problem for the past several years, the Department had not yet resolved systems inventory related weaknesses. Specifically, the Department's current systems inventory process consists of an annual data call to sites and organizations. During this process, the Department relies completely on programs and contractors to self-report their

inventory. However, the Office of the Chief Information Officer (OCIO) conducts only limited verification to check the consistency of information reported quarterly. An accurate and complete inventory of the Department's information resources is needed to plan for and institute appropriate protective measures for its systems, especially those that contain sensitive and personally identifiable information (PII).

In addition, as we reported last year, the Department had not deployed a complex-wide automated asset management tool to help track systems and identify interfaces between systems or networks. The online tool chosen as a solution by the Department, initiated in 2007, was to provide the capability to capture systems inventory information, but delays continue to push back full implementation. An OCIO official anticipated sites and programs would be required to use the new system by the third quarter of Fiscal Year (FY) 2010. Although not a Federal requirement, an automated asset management tool – when fully implemented – could assist the Department in not only FISMA reporting but also in areas such as risk management, capital planning, and configuration management.

Security Controls

While many of the security control deficiencies reported during our previous evaluation had been corrected, we issued six findings during our current review related to access controls and/or configuration management. These controls help prevent unauthorized access and modification to information systems and data from both internal and external sources. Based on our testing, we found that weaknesses in these areas existed at a number of sites. In a number of instances, site officials took action to correct weaknesses soon after we brought them to their attention. However, as described below, various weaknesses remain.

<u>Access Controls</u>

The Department continued to experience access control weaknesses for its information systems. 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. Although one site closed an access control finding identified during last year's review, we noted that control weaknesses continued to exist at multiple sites, including:

- Eight sites had default or weak account credentials such as usernames and passwords. In addition, passwords were not always changed or locked out according to Department policy. While deficiencies at six of these sites were corrected immediately after we pointed them out, the failure to fully implement corrective actions at the two remaining sites increased the risk of exposure of sensitive information to users with malicious intent. For example, the default vendor-supplied administrator user identification and password were not disabled or changed after the installation of a test system at one site. This weakness could have permitted an unauthorized user to access multiple systems by using the system administrator's user identification and password;

- Two sites had not conducted timely periodic management reviews of user accounts and related access privileges. For instance, one site had not conducted such a review in more than a year, limiting its ability to effectively monitor changes in access privileges. In another case, access levels at one site were not periodically reconciled with documented requirements. Management review of user accounts and related access privileges is essential to determining whether users who no longer have a valid need for information resources because of job changes or resignations had their access removed in a timely manner; and,

- As disclosed in our report on *Protection of the Department of Energy's Unclassified Sensitive Electronic Information* (DOE/IG-0818, August 2009), access controls over laptop computers taken on foreign travel from one site were not adequate. Specifically, logical security assessments to identify potential infections from malware were not conducted prior to accessing the site's network after returning from travel. As a result, the site's network was subjected to potential exploitation if the laptop had been compromised while on foreign travel.

<u>Configuration Management</u>

Although actions were taken to mitigate configuration management findings identified during our FY 2008 review, we identified additional weaknesses at a number of Department sites this year. These weaknesses included software vulnerabilities and deficiencies in implementing common security configurations. Configuration management controls 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. However, our review disclosed that:

- Nine sites were using outdated network services or were missing security patches, including one site where software vulnerabilities identified by the manufacturer in 2007 were not patched even though fixes were available to correct the weakness. This vulnerability could have allowed unauthorized access to system administrator functions on any of the systems running the software;

- At one site, a server containing human resources data, including PII, was connected to the network with a configuration that permitted any user on the network to access the data through an anonymous connection. During our testwork, we were able to exploit this vulnerability to obtain privacy data; and,

- Six sites used software configurations that were not secure, a practice that could result in the compromise of system administrator account credentials and ultimately allow unauthorized access to other internal systems.

In addition, numerous sites had not implemented the Federal Desktop Core Configuration (FDCC) mandated by the Office of Management and Budget. While the FDCC was designed to, among other things, make information systems more secure, we identified that seven Science field sites reviewed had implemented security configurations that were less

_____

stringent than those included in the FDCC. Furthermore, our current evaluation noted that although most Under Secretary of Energy and NNSA sites reviewed had implemented FDCC, certain sites were still working to meet the requirements. We recognize that the FDCC may not be appropriate in certain scientific or research environments and accounted for these circumstances in our review.

Cyber Security Management Program

The problems identified occurred, at least in part, because certain cyber security roles and responsibilities had not been clearly delineated. In addition, programs and sites had not effectively conducted performance monitoring of cyber security performance and ensured that Plans of Action & Milestones (POA&M) were used effectively.

<u>Coordination</u>

The OCIO and NNSA had made extensive efforts to coordinate the transition of a number of sites to the Department of Energy's Common Operating Environment (DOE-COE), an initiative launched by the Department to consolidate all aspects of common IT systems that had previously been managed separately by various organizations. However, we noted that certain roles and responsibilities related to the transition were not clearly delineated and contributed to three of the eight weaknesses identified during our review. For example, responsibility for certain areas were unclear and, therefore, some required functions were not completed while the performance of other less pressing functions were omitted altogether. In response to the weaknesses we identified, officials stated they were developing corrective action plans and expected to remedy the specific weaknesses by the end of the Fiscal Year.

<u>Performance Monitoring</u>

As noted in previous evaluations, Department management had not effectively performed monitoring and review activities essential for evaluating the adequacy of cyber security performance and had not ensured that POA&Ms were always used effectively. For example, certain program-level cyber security representatives stated that a lack of resources prevented them from performing effective oversight within their respective programs. As such, they relied on reviews conducted by the OIG, Government Accountability Office, and HSS to help with monitoring activities and address related

cyber security weaknesses. While these independent organizations may make recommendations for improving controls, the reviews they perform are not a substitute for an effective internal control and management review structure. Rather, management is responsible for providing adequate oversight.

Furthermore, despite concurring with previous OIG recommendations, NNSA had not fully implemented an adequate periodic evaluation mechanism to ensure the effectiveness of field sites in carrying out their responsibilities for proper implementation of Federal cyber security requirements. NNSA informed us during the course of our evaluation that it had developed an aggressive assessment schedule for FY 2010 that, if adhered to, should further enhance its performance monitoring program.

As with past reviews, we identified problems regarding the use of POA&Ms as a management tool for tracking and correcting all known cyber security weaknesses. In particular:

- Although the Department was working to implement corrective actions, five of nine cyber security weaknesses identified during our FY 2008 evaluation were not included in the Department's POA&M;

- Our evaluation identified that POA&Ms did not contain all cyber security weaknesses identified by oversight organizations, including numerous security related OIG reports; and,

- We identified that about seven percent of open milestones captured in the POA&Ms were at least one year beyond their projected remediation date, including one that was more than four years beyond its target date.

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.

Resources and Data Remain at Risk

During FY 2009, the Department took a number of steps designed to improve its cyber security program. However, weaknesses continue to exist in key areas. As demonstrated by recent HSS penetration testing, Departmental systems and

_____

information remain vulnerable to attack and exploitation. Specifically, HSS was able to gain access to large network segments at two national laboratories managed by Science and exfiltrated significant quantities of sensitive information, including PII. Notably, at least two other sites detected the attack and prevented HSS from gaining network access.

The importance and need for sustained action is well demonstrated by industry experts who report that the number of new malicious code threats increased over 1,000 percent from 2006 to 2008. The Department also reported a 39 percent increase in the number of total incidents between FYs 2008 and 2009. While this increase may represent enhanced reporting, it also demonstrates the need to continuously improve detection capabilities and cyber security awareness. In addition, the Department reported that the number of attempted intrusions of its networks had increased rapidly between 2006 and 2008. As such, sites must remain vigilant if they are to maintain their ability to thwart potential attacks from internal and external threats.

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 cognizant program elements, as appropriate:

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

2. Ensure effective coordination of efforts and responsibilities between the OCIO and programs during DOE-COE implementation at field sites;

3. Perform compliance monitoring activities to ensure the adequacy of cyber security program performance; and,

4. Ensure that POA&Ms are complete and are utilized as a management tool for prioritizing corrective actions and tracking all known cyber security weaknesses to completion.

MANAGEMENT REACTION

Management concurred with each of the report's recommendations and provided technical comments on the content of the report. Management added that it had initiated or completed corrective actions designed to address weaknesses identified during our review. Management noted that it continues to focus attention on coordination efforts related to DOE-COE implementation. In addition, management disclosed that it continues to work towards automating the complex-wide FISMA reporting process.

In separate comments, the NNSA did not specifically indicate whether it agreed with our recommendations. However, NNSA disclosed that it generally agreed with the report content, but requested more specificity in certain areas. In addition, NNSA commented that it did not agree with the report finding that it had not fully implemented an adequate periodic evaluation mechanism. NNSA added that it was working to procure and deploy an asset management tool as part of its overall continuous monitoring program.

AUDITORS COMMENTS

Management's comments were responsive to our recommendations. However, because the NNSA did not indicate whether it agreed with our recommendations, we consider NNSA's comments to be non-responsive. Regarding NNSA's comment that greater specificity is needed in the report, NNSA Headquarters and Site Office officials were provided with a copy of each of the findings related to its program during our review. NNSA concurred with all but one of the findings, which has since been closed and is not discussed in this report. In addition, NNSA provided corrective action plans in response to each of the findings. Although NNSA's comments disclosed that it did not agree with the report finding related to implementation of an adequate periodic evaluation mechanism, NNSA specifically concurred with our finding and recommendation related to this area at the time of our review. Management's and NNSA's comments are included in their entirety in Appendix 3.

OBJECTIVE
To determine whether the Department of Energy's (DOE or Department) unclassified cyber security program adequately protected data and information systems.

SCOPE
The evaluation was performed between February 2009 and September 2009 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 Health, Safety and Security Office of Independent Oversight performed a separate evaluation of the Department's information security program for National Security Systems.

METHODOLOGY
To accomplish the audit objective, we:

- Reviewed applicable laws and directives pertaining to cyber security and information technology resources such as the *Federal Information Security Management Act of 2002*, 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 (KPMG), the Office of Inspector General (OIG) contract auditor. KPMG work included analysis and testing of general and application controls for systems as well as vulnerability and penetration testing of networks; and,

_____

Objective, Scope and Methodology

- Reviewed and incorporated the results of other cyber security review work performed by the OIG, 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

- *Protection of the Department of Energy's Unclassified Sensitive Electronic Information* (DOE-IG-0818, August 2009). Opportunities exist to strengthen the protection of all types of sensitive unclassified electronic information. For example, sites: had not ensured that sensitive information maintained on mobile devices was encrypted or they had improperly permitted sensitive unclassified information to be transmitted unencrypted through email or to offsite backup storage facilities; had not ensured that laptops taken on foreign travel were protected against security treats; and, were still working to complete required Privacy Impact Assessments.

- *Management Challenges at the Department of Energy* (DOE/IG-0808, December 2008). The Office of Inspector General (OIG) identified six significant management challenges facing the Department of Energy (Department), including cyber security. Although the Department had made improvements in its unclassified cyber security program, the OIG continued to identify deficiencies relevant to certification and accreditation (C&A) of systems, contingency planning, systems inventory, and segregation of duties.

- *Cyber Security Risk Management Practices at the Bonneville Power Administration* (DOE/IG-0807, December 2008). Bonneville had not always appropriately identified and addressed potential risks to critical systems and data, to include systems controlling electricity transmission; developed adequate security plans for each of the four systems reviewed; ensured that physical and cyber security controls were tested and operating as intended; and, developed corrective action plans necessary to resolve weaknesses in a number of important control areas.

- *Cyber Security Risk Management Practices at the Southeastern, Southwestern, and Western Area Power Administrations* (DOE/IG-0805, November 2008). These Power Marketing Administrations had not always developed adequate security plans for each of the 12 systems reviewed; ensured that physical and cyber security controls were tested and operating as intended; developed corrective action plans necessary to resolve weaknesses in a number of important control areas; and, developed contingency plans to ensure that systems could be recovered in the event of a significant outage.

- *The Department's Unclassified Cyber Security Program - 2008* (DOE/IG-0801, September 2008). The review identified opportunities for improvements in areas such as C&A of systems; systems inventory; contingency planning; and, segregation of duties. Similar to past observations, these internal control weaknesses existed, at least in part, because not all Department program organizations, including the National Nuclear Security Administration (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. Risk of compromise to the Department's information and systems remained higher than necessary.

- *The Department's Unclassified Foreign Visits and Assignments Program* (DOE/IG-0791, March 2008). Not all NNSA 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 settings, loading unauthorized software, removing software, and changing computer settings. Some foreign visitors and assignees had unsupervised use of their foreign government, university, or business laptops within laboratory facilities which had live Intranet connections.

- *Management of the Department's Publicly Accessible Websites* (DOE/IG-0789, March 2008). Some of the Department's publicly accessible websites did not meet Federal accessibility requirements or contingency planning. Content on publicly accessible web servers was not always controlled and reviewed periodically. This resulted in eight instances that involved personally identifiable information (PII) being exposed to unauthorized or malicious sources. 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.

- *The Department's Cyber Security Incident Management Program* (DOE/IG-0787, January 2008). Program elements and facility contractors 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, despite identifying and acknowledging weaknesses in its cyber security incident management and response program.

- *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, not detained by cyber security personnel, and the written incident report was not completed within 32 hour reporting requirement. An additional 37 laptop computers may have been improperly introduced into the Limited Area by Oak Ridge National Laboratory personnel in recent years with these incidents not properly reported in a timely manner.

- *The Department's Unclassified Cyber Security Program - 2007* (DOE/IG-0776, September 2007). Problems persisted with the C&A of the Department's systems related to assessing risks and ensuring the adequacy of security controls. The Department had not established a complex-wide inventory systems 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. Risk of compromise to the Department's information and systems remains higher than acceptable.

- *Security Over Personally Identifiable Information* (DOE/IG-0771, July 2007). The Department had not identified all site-level systems containing PII or evaluated the risks associated with maintaining such systems; remote access protection measures had not been fully deployed in accordance with Departmental direction; and, some sites had not identified mobile computing devices containing PII nor ensured that such information was encrypted.

- *The Department's Efforts to Implement Common Information Technology Services at Headquarters* (DOE/IG-0763, March 2007). Five major organizations, 40 percent of the total potential user population, were not migrated to the Department's Common Operating Environment within the first year as planned, thereby preventing realization of the full $15 million of first year savings. For certain organizations in which implementation was completed, services were not disabled for terminated employees in a timely manner, resulting in the payment of over $700,000 in unnecessary user fees and creating potential cyber security vulnerabilities.

- *Excessing of Computers Used for Unclassified Controlled Information at Lawrence Livermore National Laboratory* (DOE/IG-0759, March 2007). NNSA delayed having Lawrence Livermore National Laboratory (LLNL) implement Departmental policy on clearing, sanitizing, and destroying memory devices for almost two and a half years after the policy was issued while its Office of the Chief Information Officer (OCIO) drafted a policy letter to provide NNSA sites with specific requirements. This delay caused LLNL to not establish certain site-wide procedures and internal controls necessary to ensure the proper clearing, sanitizing, and destroying of unclassified controlled information on electronic memory devices.

- *The National Nuclear Security Administration's Implementation of the Federal Information Security Management Act* (DOE/IG-0758, February 2007). NNSA did not always properly implement its own guidance as well as Departmental and Federal cyber security requirements and had not performed regular monitoring activities essential to evaluating the adequacy of cyber security program performance. Therefore, 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.

- *Certification and Accreditation of Unclassified Information Systems* (DOE/IG-0752, January 2007). Many of the Department's systems were not properly certified and accredited prior to becoming operational. For example, 9 of 14 sites reviewed did not properly access 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. The OCIO and program elements did not adequately review completed activities for quality or compliance with requirements.

Government Accountability Office Reports

- *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses* (GAO-09-546, July 2009)

- *Federal Information Security Issues* (GAO-09-817R, June 30, 2009)

- *Cybersecurity: Continued Federal Efforts are Needed to Protect Critical Systems and Information* (GAO-09-835T, June 25, 2009)

- *Information Security: Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist* (GAO-09-701T, May 19, 2009)

- *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk* (GAO-09-661T, May 5, 2009)

- *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture* (GAO-09-432T, March 10, 2009)

- *Nuclear Security: Los Alamos National Laboratory Faces Challenges In Sustaining Physical and Cyber Security Improvements* (GAO-08-1180T, September 25, 2008)

- *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network* (GAO-08-1001, September 2008)

- *Los Alamos National Laboratory: Long-Term Strategies Needed to Improve Security and Management Oversight* (GAO-08-694, June 2008)

- *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist* (GAO-08-571T, March 12, 2008)

- *Information Security: Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies* (GAO-08-496T, February 14, 2008)

- *Information Security: Protecting Personally Identifiable Information* (GAO-08-343, January 2008)

- *National Nuclear Security Administration: Security and Management Improvements Can Enhance Implementation of the NNSA Act* (GAO-07-428T, January 31, 2007)

- *National Nuclear Security Administration: Additional Actions Needed to Improve Management of the Nation's Nuclear Programs* (GAO-07-36, January 2007)

Office of Health, Safety and Security Reports

- *Independent Oversight Inspection of the Unclassified Cyber Security Program at the National Training Center*, June 2009

- *Independent Oversight Inspection of the Office of Environmental Management Classified and Unclassified Cyber Security Programs at the Savannah River Site*, March 2009

- *Independent Oversight Unclassified Cyber Security Inspection of the Idaho Operations Office, the Idaho National Laboratory, and the Idaho Cleanup Project*, March 2009

- *Independent Oversight Unclassified Cyber Security Inspection of the Southeastern Power Administration*, February 2009

- *Independent Oversight Unclassified Cyber Security Inspection of the Princeton Plasma Physics Laboratory*, November 2008

- *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.

Department of Energy
Washington, DC 20585

September 28, 2009

MEMORANDUM FOR GREGORY H. FRIEDMAN
INSPECTOR GENERAL

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

SUBJECT: Draft Evaluation Report on "The Department's
Unclassified Cyber Security Program – 2009"

Thank you for the opportunity to comment on this draft report. The Office of the CIO (OCIO) appreciates very much the effort that has gone into this report, including the recognition of the Department's incremental progress over the past year in enhancing its unclassified cyber security program and in addressing previously identified weaknesses. The information in this report will enable OCIO and program offices to take appropriate follow-up action on specific findings.

With respect to the specific recommendations in this draft report:

Recommendation 1: That the Department and the NNSA Chief Information Officers, in conjunction with the cognizant program elements as appropriate, *correct, through the implementation of management, operational, and technical controls, each of the specific vulnerabilities identified in this report.*

Concur. The specific issues identified in this report have been identified throughout the current and prior years in site and program evaluations and audits. Plans of Action and Milestones (POA&Ms) have been created, and the corrective actions cited in response to each of the Office of Inspector General's previously issued evaluations and reports are underway. In some cases, corrective actions have already been completed since this draft report was prepared.

Recommendation 2: That the Department and the NNSA Chief Information Officers, in conjunction with the cognizant program elements as appropriate, *ensure effective coordination of efforts and responsibilities between the OCIO and programs during DOECOE implementation at field sites.*

Concur. OCIO has consistently recognized the importance of establishing effective program management relationships while deploying the Department of Energy Common Operating Environment (DOECOE). An important part of this coordination involves cyber security, including coordination of responsibilities on the part of the programs and OCIO. Special attention is being given to site cyber security concerns recognized prior to the transition to DOECOE that need to be carried forward by the program or OCIO. The execution of DOECOE Service

Printed with soy ink on recycled paper

Level Agreements will solidify and reconfirm the roles and responsibilities between OCIO and the programs.

Recommendation 3: That the Department and the NNSA Chief Information Officers, in conjunction with the cognizant program elements as appropriate, *perform compliance monitoring activities to ensure the adequacy of cyber security program.*

Concur. All programs must continue to perform adequate and appropriate compliance monitoring activities to ensure effective cyber security operations. OCIO will continue to perform appropriate compliance monitoring, and OCIO will work with the programs to identify cyber security activities that programs should consider including in their program cyber security compliance monitoring processes.

Recommendation 4: That the Department and the NNSA Chief Information Officers, in conjunction with the cognizant program elements as appropriate, *ensure that POA&Ms are complete and are utilized as a management tool for prioritizing corrective actions and tracking all known cyber security weaknesses to completion.*

Concur. OCIO, working with the programs, will continue to deploy automated C&A and FISMA reporting modules that are expected to improve accuracy and ease of reporting, including creation of POA&Ms. However, updating and tracking of POA&Ms will still rely on sustained program management attention to remediation of identified weaknesses, and must have the active involvement of Designated Approving Authorities. OCIO will assist headquarters-level program management in their use of the automated FISMA reporting module to improve their tracking of corrective actions within their programs.

If you need additional information, please contact Bill Hunteman, Associate CIO for Cyber Security at (202) 586-4775. Technical attachments are provided in an attachment to this memorandum.

Attachment

NNSA
National Nuclear Security Administration

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

OCT ---6 2009

MEMORANDUM FOR   George W. Collard
Assistant Inspector General
for Performance Audits

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Comment to Draft 2009 Cyber Security Report; A07TG035;
IDRMS No. 2009-00103

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report, *The Department's Unclassified Cyber Security Program - 2009*. We understand that the IG wanted to determine whether the Department's Unclassified Cyber Security Program adequately protected data and information systems.

As an Agency, it would be beneficial if the IG would issue a separate report to NNSA with specificity as to anomalies associated with our sites. While we work closely with the Department's Chief Information Officer, NNSA has policies, plans, and procedures for its complex that differ from non-NNSA elements of the Department.

NNSA generally agrees with the report. However, there are areas where specificity will be helpful in corrective action planning. These areas are:

1. NNSA's main concern is that there are many references to many findings throughout the report, but there is no clear indication as to what organization these findings were issued against. The report is written in a generic fashion and, as a result, is difficult to interpret. NNSA would appreciate greater specificity and clarity in the report as the audit was not performed against any one specific organization.

2. The first paragraph on page 1, Program Improvements, contains six bullets. It is not clear whether these bullets are actions that NNSA took to mitigate prior weaknesses or if these bullets are an overall combination of mitigation actions taken by other organizations also mentioned in this paragraph. There is also a reference to two prior findings for NNSA that have not been resolved, however the two findings are not specifically identified in this report.

3. We concur with the finding that most NNSA sites had implemented FDCC but there are still some sites working to meet the requirement.

2
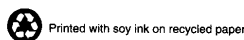
4. The report fails to clarify references to a lack of coordination between NNSA and the DOE OCIO for the deployment of DOECOE. The report mentions that roles and responsibilities for certain areas were unclear but greater specificity is needed to determine this lack of coordination. It is not clear whether this finding is written against the NNSA, DOE OCIO, or both.

5. The Performance Monitoring section states that the periodic evaluation mechanism for field sites within NNSA is inadequate. NNSA assumes that this is referring to the Security Engineering Board (SEB). If this is the case, NNSA disagrees with this statement. The SEB is under the leadership of a federal lead and conducts complete assessments of all NNSA sites. All assessments completed are provided to the IG for feedback. To date, we have not received any feedback on the reports provided to the IG.

6. The Department was cited for not having deployed a complex-wide asset management tool. NNSA is currently working to procure and deploy an asset management tool as part of our overall continuous monitoring program.

NNSA will provide corrective actions to the recommendations during the Management Decision phase.

Should you have any questions about this response, please contact JoAnne Parker, Acting Director, Policy and Internal Controls Management at 202-586-1913.

cc: Linda Wilbanks, Chief Information Officer
        David Boyd, Senior Procurement Executive
        Karen Boardman, Director, Service Center

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 Felicia Jones at (202) 253-2162.

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.