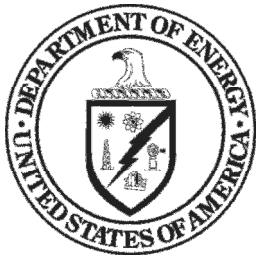

U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Evaluation Report

The Department's Unclassified Cyber Security Program – 2010

DOE/IG-0843 October 2010

Department of Energy
Washington, DC 20585

October 22, 2010

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department's Unclassified Cyber Security Program - 2010"

BACKGROUND

Federal information systems are routinely confronted with increasingly sustained cyber attacks – many of which involve targeted and serious threats – executed with varying levels of technical sophistication. The number of incidents reported by Federal agencies to the Department of Homeland Security has, in fact, increased by over 400 percent in the past 4 years. To help combat the escalating number and complexity of cyber security threats, the Department of Energy expended significant funds in Fiscal Year (FY) 2010 on cyber security measures designed to protect systems and their information. The Department's systems support various program operations, including its energy, national security, scientific discovery and innovation, and environmental remediation portfolios.

The Federal Information Security Management Act of 2002 (FISMA) provides direction on the development, implementation and management of an agency-wide information security program to provide protection commensurate with risk for Federal information and systems, including those managed by another agency or contractors. In accordance with FISMA, the Office of Inspector General conducted its annual independent evaluation to determine whether the Department had adopted a risk-based cyber security program that adequately secured its unclassified information and systems. The attached report presents the results of our evaluation for FY 2010.

RESULTS OF EVALUATION

Our evaluation disclosed that the Department had taken steps to enhance its unclassified cyber security program, including resolving five of seven cyber security weaknesses identified during our FY 2009 evaluation. In addition, the Department had initiated implementation of an automated tool to aid in security and performance reporting. The Department also continued to maintain its defense-in-depth strategy to protect its networks against intruders and other external threats.

While these were positive accomplishments, additional action is needed to further strengthen the Department's unclassified cyber security program and help mitigate threats to its information and systems. In this context, our review revealed weaknesses in the areas of access controls, configuration and vulnerability management, web application integrity, and security planning and testing. Specifically:

- At five locations, we noted vulnerabilities related to access controls such as weak or blank system administrator passwords and a lack of periodic account reviews;

- Weaknesses existed in the area of system configuration and vulnerability management at 12 locations. These issues included outdated security patches on desktops and network servers, as well as the use of default or weak security settings – situations that could allow unauthorized access to system resources;

- Six locations had weaknesses in web applications, vulnerabilities which could be exploited to launch attacks against users or host systems; and,

- A Headquarters program office placed a system into operation prior to completing required system security plans and related testing of controls.

The weaknesses identified occurred, at least in part, because Departmental elements had not always ensured that cyber security requirements were effectively implemented. In addition, the Department (including the National Nuclear Security Administration) had not adequately monitored cyber security performance. Plans of action and milestones were also not always used effectively to ensure that known security vulnerabilities were properly remediated. Without improvements to its cyber security program, Departmental systems and the information they contain are exposed to a higher than necessary level of risk. While all identified vulnerabilities were discussed with cognizant officials to determine their potential effect, the scope of our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

In light of the growing number of cyber security threats and the noted vulnerabilities, we made several recommendations designed to help the Department strengthen its unclassified cyber security program. When fully implemented, these should help the Department adequately protect its systems and data from the threat of compromise, loss, or inappropriate modification and non-availability.

Due to security considerations, information on specific vulnerabilities and locations has been omitted from this report. Throughout the evaluation, however, we closely coordinated all findings with applicable Federal and contractor officials. During these interactions, site and program officials were provided with detailed information regarding respective vulnerabilities identified. We also obtained information regarding the applicability of our findings to each respective risk environment. In many instances, corrective actions to address these findings were initiated immediately.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that corrective action would be taken. However, management expressed concern with our characterization of the scope, severity and cause of the issues discussed within the report. Management's comments and our response are more thoroughly discussed in the body of the report and are included in Appendix 3.

Attachment

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

EVALUATION REPORT ON THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM – 2010

TABLE OF CONTENTS

Department's Unclassified Cyber Security Program

Appendices

The Department's Unclassified Cyber Security Program – 2010

Program Improvements

The Department of Energy (Department) had taken positive steps to address previously identified cyber security weaknesses and enhance its unclassified cyber security program. We noted that corrective actions had been taken to resolve five of seven weaknesses identified during our evaluation of *The Department's Unclassified Cyber Security Program - 2009* (DOE/IG-0828, October 2009). Specifically:

- The National Nuclear Security Administration (NNSA) had taken action to address previously identified weaknesses. For instance, certain sites implemented plans designed to help resolve remote system management issues. In addition, two sites established procedures and practices for minimizing risks from configuration management vulnerabilities;

- The Department established a new Computer Security Governance Council at the Under Secretary level to lead the Department's cyber security reform initiatives. The Council is supported by a new Computer Security Advisory Group, which is composed of senior information technology (IT) and cyber security representatives from each of the Department's major components;

- In August 2010, the Department began the formal vetting process for Draft Order 205.1B – *Department of Energy Cyber Security Program* – to update, define, and establish its new cyber security management structure and realign the cyber security program with a more risk-based approach; and,

- The Department initiated actions to transform its risk management framework by implementing the TrustedAgent™ system to automate and standardize reporting requirements and deploy continuous monitoring tools in support of the Federal Information Security Management Act of 2002 (FISMA).

Security Controls and Risk Management

The Department had made progress in addressing technical control weaknesses identified during our previous evaluation. However, during our current review, we identified various issues at sites managed by the NNSA, Under Secretary for Science, and Under Secretary of Energy that involved the implementation of technical controls. Specifically, we

identified problems in the areas of access controls, configuration and vulnerability management, and integrity of web applications at 15 of 17 locations. In a number of instances, site officials took action to correct certain weaknesses shortly after we identified them. However, as detailed in the remainder of our report, various weaknesses remained. Furthermore, our review disclosed risk management weaknesses related to security planning and testing of certain information systems.

Access Controls

Despite efforts to correct previously identified problems, the Department continued to experience access management weaknesses. 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 must be strong and functional. Although action had been taken to address one of two access control issues identified last year, one remained unresolved. Furthermore, eight new problems related to access controls were revealed by this year's testing. In particular:

- One site had access control weaknesses that affected logical, physical and personnel security. Specifically, the site had not developed and/or implemented adequate policies and procedures to ensure controls over these access categories were in place. For instance, we noted that formal processes did not always address essential elements such as safeguards over granting privileged users logical and physical access to IT resources, or ensuring that user access was removed upon termination of employment;

- Two sites had network systems and devices with administrator level accounts that were configured with default, blank or easily guessed passwords. While deficiencies at these sites were corrected immediately after we pointed them out, weaknesses in the process for identifying such accounts could have permitted an unauthorized user to access multiple systems;

- Three locations had not always effectively conducted periodic reviews of user accounts and related access privileges. In one case, the site had not corrected issues

identified during our previous evaluation and had granted incompatible access levels to system developers and a system administrator. At two other sites, officials had not always performed effective periodic management reviews of user accounts and related access privileges. Although one site performed bi-annual reviews, these were not conducted in a timely manner and failed to identify inappropriate access privileges for two users. Management review of user accounts is essential to determining whether users who no longer have a valid need to access system resources have their privileges removed in a timely manner;

- One site had not adhered to the requirement to change passwords every 180 days in accordance with National Institute of Standards and Technology (NIST), Department, and site-level password standards and directives. Specifically, a password for its human resources system's default privileged account had not been changed within the established timeframe nor did the site's financial system enforce password changes as required; and,

- One site maintained a File Transfer Protocol server that accepted anonymous connections and could have allowed any user to gain access to files, including those containing valid usernames and passwords for other systems.

Configuration and Vulnerability Management

Although corrective actions had been taken to resolve configuration management vulnerabilities identified in our Fiscal Year (FY) 2009 evaluation, weaknesses in these areas persisted. In particular, problems discovered during our current review were attributed to inadequate configuration and vulnerability management controls. Performance testing revealed that all 17 locations reviewed had varying degrees of vulnerable applications on desktop and network systems and devices. Specifically, we found that:

- Twelve locations had desktop systems with known vulnerabilities that had not been corrected by installing current security patches. Based on a NIST assessment tool, the missing security patches were classified as "high risk" and we noted that they had been available

for at least 3 months prior to our testing. The failure to apply these patches could have permitted unauthorized access to system administrator functions;

- We also found that four locations failed to properly patch network server systems and devices. As with the desktop systems previously discussed, security patches for known vulnerabilities had been released more than 3 months prior to our testing. Vulnerable applications included database servers, web servers, and various other network services; and,

- Two sites had instances of network devices with default or weak settings. These weaknesses could have allowed unauthorized users to modify configuration settings or anonymously read shared directories and files, including files containing employees' personally identifiable information and login credentials for other systems. As a result, it was possible for an authenticated user to access sensitive data stored on the server.

Some of the identified vulnerabilities affected systems and other servers hosting financial and non-financial systems, problems that could have permitted individuals to gain administrator level access. At certain sites, the risk associated with these weaknesses was mitigated, in part, by the existence of network-based compensating controls that help to ensure that malicious attacks with known exploit signatures would not be delivered to a vulnerable system. However, exploit of these vulnerabilities by a malicious user could have resulted in an immediate or indirect compromise of business information or unauthorized access to key application functionality and data, as well as loss or disruption of critical operations.

Integrity of Web Applications

The Department experienced system and data integrity deficiencies on several web applications used to support activities such as human resources, property management and medical applications. Specifically, our performance testing identified at least 10 web-based applications at 6 locations that did not perform validation procedures. System and data integrity controls ensure that changes made to information and programs are allowed only in a specified and authorized manner and that the system performs intended functions in an

unimpaired manner free from deliberate or inadvertent unauthorized manipulation of the system, such as through software flaws and malicious code. However, we found that:

- Five locations operated applications that accepted malicious input data that could have then been used to launch attacks against legitimate application users or result in unauthorized access to the application; and,

- One site maintained a medical information application that did not always perform validation procedures to determine whether data parameters had been modified by a user. By modifying parameters, an authenticated user could view or modify another user's privacy data. Following our review, site officials commented that they had taken corrective action to address the identified weaknesses.

Security Planning and Testing

Our review also disclosed risk management weaknesses related to security planning and testing of certain systems. This process is essential for ensuring a complete and effective risk management strategy for protecting IT systems and the data they contain. Specifically, during our reviews of two systems operated by the Department's Office of Energy Efficiency and Renewable Energy, we identified weaknesses related to incomplete security control planning and testing that could have aided in managing the risks associated with deployment and operation of the systems. Security planning and testing are critical activities that support the risk management process and are integral to the agency's information security program. In particular:

- Our report on *Management Controls over the Development and Implementation of the Office of Energy Efficiency and Renewable Energy's Performance and Accountability for Grants in Energy (PAGE) System* (OAS-RA-10-14, July 2010) revealed that the system was placed into operation before required cyber security planning and testing was completed. The lack of planning and testing placed the PAGE system and the network on which it resided at increased risk that the confidentiality, integrity and availability of the Department's information systems and data could be compromised; and,

- Our audit of *Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act* (OAS-RA-10-05, March 2010) identified that the system's security planning documentation and control testing was incomplete and inconsistent. For example, the information contained in the system security plan was not representative of the entire computing environment. In addition, a significant portion of the required security controls had been excluded from testing. These weaknesses exposed the system and data to a higher than necessary level of risk of compromise, loss, modification, and non-availability.

Implementation of Requirements and Performance Monitoring

The weaknesses identified occurred, at least in part, because Departmental elements had not always ensured that cyber security requirements were effectively implemented. In addition, Department programs and the NNSA had not adequately conducted cyber security performance monitoring activities. Plans of action and milestones (POA&Ms) were also not used effectively to ensure that known security vulnerabilities were remediated.

Procedures and Processes

Programs and sites reviewed had not always implemented policies and procedures designed to ensure that minimum cyber security standards were met. For instance, we noted that site-level policies and procedures were not fully effective in areas such as configuration and vulnerability management. Even when procedures were established and being used, sites had not always verified, through testing or by other means, that the procedures were effective. Furthermore, access control policies and procedures were not always developed and/or implemented. At one site, we noted that formal policies and procedures did not exist for various access control activities, including authorizing, reviewing and terminating access to certain systems or conducting periodic reviews of user access accounts. In addition, we found that web application functionality at certain locations was developed without an adequate process in place to ensure effective controls were implemented. This weakness could have allowed individuals to launch attacks against legitimate application users or result in unauthorized access to the application.

Performance Monitoring

Consistent with our findings of previous years, Department and NNSA management had not effectively conducted monitoring and review activities essential for evaluating cyber security performance. For example, we noted that NNSA Headquarters officials still had not fully instituted a process for evaluating the activities of Federal site offices and associated field sites. In addition, we identified problems with the Department's use of POA&Ms as a management tool for tracking, reporting and correcting known security vulnerabilities.

During our review, we noted that NNSA management instituted a moratorium on internal reviews, including cyber security assessments, for a large portion of the fiscal year. As a result, only one unclassified assessment had been completed by Headquarters officials. The lack of assessments was of particular concern because the Department and NNSA are working to revise their oversight approach to rely largely on the contractor assurance system model, which will define and provide a mechanism by which management can assess contractor performance within an established risk management framework. In our judgment, ensuring that an adequate oversight framework is in place is essential if the contractor assurance model is to work in a credible and effective manner.

Consistent with prior reviews, we continued to identify problems with the Department's use of POA&Ms as a management tool to report, prioritize and track cyber security weaknesses through remediation. Specifically, we found instances where:

- POA&Ms did not contain all identified cyber security weaknesses for unclassified information systems. For example, although corrective actions had been initiated or completed, we noted that four cyber security weaknesses found during our FY 2009 evaluation had not been included in the Department's POA&M. In one instance, a site that was issued a finding for the second consecutive year regarding weak password management controls still had not included corrective actions in the POA&M;

- Our evaluation identified 113 (12 percent) open milestones captured in the POA&M that were beyond

their projected remediation date. In a few instances, we noted that open milestones were at least one year beyond their estimated remediation date; and,

- We also found that 71 (8 percent) open milestones had no associated funding included in the POA&M. A lack of estimates related to the cost of remediating weaknesses limits the ability of responsible officials to effectively prioritize corrective actions.

As pointed out by NIST and as reiterated by the Office of Management and Budget (OMB), POA&Ms are an important means of identifying and managing an entity's progress towards eliminating gaps between required security controls and those that are actually in place.

Information and Systems Remain at Risk

Without improvements to its cyber security program, such as adherence to required risk management practices and the adoption of processes to ensure that security controls are fully implemented, Department systems and the information they contain continue to be exposed to a higher than necessary level of risk of compromise, loss, modification and non-availability.

Our testing at 17 locations identified many vulnerabilities – each of which were reviewed for severity and discussed with site officials. As a result, many of the weaknesses identified were not included in this report because we concluded that existing risk assessments or compensating controls were adequate. Although we found that many sites had implemented compensating controls, such as anti-malware applications, to mitigate the risk associated with certain vulnerabilities, an attacker could potentially execute attacks against certain vulnerable systems, key applications, and user desktops by using custom attacks with no known signatures. Exploitation by unauthorized or malicious individuals could also lead to disruption of operations, modification or destruction of sensitive data or programs, or theft or improper disclosure of confidential business information.

As reported by the Department of Homeland Security, Federal information systems continue to be confronted with increasingly pervasive and sustained cyber attacks that have evolved into more targeted and serious threats with varying levels of access and technical sophistication. Further, without improvements in the Department's POA&M process, management may be unaware of, or unable to effectively

prioritize the remediation of existing vulnerabilities and security weaknesses. This lack of awareness could potentially lead to insufficient resources being allocated to mitigate the system and security vulnerabilities.

RECOMMENDATIONS

To improve the effectiveness of the Department's unclassified cyber security program and to remedy the weaknesses identified in this report, we recommend that the Administrator, National Nuclear Security Administration, Under Secretary of Energy, and Under Secretary for Science, in coordination with the Department and NNSA Chief Information Officers, where appropriate:

1. Correct, through the implementation of appropriate controls, the weaknesses identified within this report;

2. Ensure that procedures and processes are developed, as needed, and are effectively implemented to adequately secure systems and applications;

3. Implement an adequate compliance monitoring program, such as the use of periodic evaluations by Headquarters management, to ensure the effectiveness of cyber security program performance; and,

4. Ensure that POA&Ms are fully developed and utilized to track, prioritize and enable remediation of identified cyber security weaknesses.

MANAGEMENT REACTION AND AUDITOR COMMENTS

Department and NNSA management concurred with the report's recommendations and stated that it had initiated corrective actions to address each of the recommendations included in our report. For instance, management stated that the Department's Cyber Security Governance Council recently approved a recommendation to implement a mission centric, risk-based approach in the management of the Department's cyber security program. In addition, NNSA management stated that it implements a flexible, comprehensive, and risk-based cyber security program. NNSA also noted that all systems were protected by distinctive, layered, and defense-in-depth approaches and that substantive risks to systems at one site almost certainly present no or extremely limited risks to systems at other sites.

Although management agreed with our recommendations, it expressed concern with our characterization of the scope, severity and cause of the issues discussed within the report.

We have summarized management's comments and provided our response for each. Management's comments are included in their entirety in Appendix 3.

Department management commented that data gathered from vulnerability scanning was not itself sufficient for making management decisions, but noted that it leveraged vulnerability scan data and other inputs, along with risk assessments, when making decisions. Management also noted that findings resulting from vulnerability scanning should not be equated with risk. We agree that vulnerability scanning is only one part of an effective defense-in-depth security strategy. However, the weaknesses included in our report were identified as "high-risk" vulnerabilities in accordance with the National Vulnerability Database sponsored by the Department of Homeland Security's National Cyber Security Division / US-CERT. In addition, we provided the results of our scans and consulted extensively with local site officials to confirm that these issues represented actual vulnerabilities and were worthy of correction. As such, the Department should utilize the results of our review to aid in developing and implementing an effective risk-management strategy that includes remediation of "high-risk" weaknesses.

Department and NNSA management commented that finding a relatively small number of misconfigured devices at the sites reviewed did not inherently suggest widespread weaknesses of control. Management also stated that the weaknesses identified in our report did not account for compensating controls and may have been within the sites' acceptable risk. NNSA commented that, although the Office of Inspector General identified a small number of systems that were determined to be misconfigured, it was important to recognize that each site was operating within its risk acceptance model. We agree that the results of our vulnerability assessment cannot be projected across the Department and, as such, did not attempt to do so in our report. However, as noted in the report, our testwork revealed weaknesses that could, if exploited, have permitted a malicious user to compromise systems or data. In fact, contrary to management's assertions, we fully considered site-level risk assessments and compensating controls. As such, many of the vulnerabilities identified during our evaluation were not included in the report based on our discussions with site officials related to their acceptance of risk and related compensating controls.

Department management commented that systems are protected by a defense-in-depth approach and noted that a technical misconfiguration should not be construed as representing substantial risk to the Department as a whole. We agree that vulnerabilities may represent differing levels of risk to various sites. In addition, because of the defense-in-depth approach implemented across the Department, we agree that a vulnerability identified at one site would not necessarily increase the risk to another site or the Department as a whole. However, the weaknesses included in our report were considered "high-risk" vulnerabilities that should be addressed locally to help reduce the threat of compromise to affected information systems and the data they contain.

Management commented that the Department's operations are complex and managed by management and operating (M&O) contractors with unique operating relationships. As such, management believed that variation and normal error could be expected. While we agree, our review revealed that many of the weaknesses identified were the result of ineffective implementation of processes and procedures by M&O contractors at the field sites. As far as we could determine, the issues identified did not necessarily relate to the complexity of the relationship between M&O contractors and the Department.

Department management commented that its goal was to improve the cyber security program and better protect the missions of the Department. We fully concur with this goal. To that end, we worked closely with officials at each of the sites we visited and provided them with detailed results of our vulnerability scanning. We also vetted each of the identified vulnerabilities extensively with site officials prior to including them in our report. Furthermore, information related to each of the weaknesses identified was provided to program officials at Headquarters throughout the course of the evaluation with the goal of helping them manage their respective cyber security programs.

Department and NNSA management comments indicated that POA&M's do not need to have budget amounts associated with them because M&O contractors are responsible for allocating funding for cyber security and other priorities based on risk management principles. Management also noted that the Department does not expect local oversight to be responsible for finding each misconfiguration or error. We believe that the amount of funding required to remediate a weakness – which is

a requirement of the OMB – can enable management to make better informed decisions related to addressing weaknesses. Furthermore, while we would not expect local oversight officials to identify every misconfiguration or error, the oversight process should include an aspect of ensuring that sites are following established policies and procedures. However, as noted in our report, we found that in many cases M&O contractors at the sites reviewed were not following existing procedures, factors which contributed to many of the issues identified.

Appendix 1

OBJECTIVE

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

SCOPE

The evaluation was performed between February 2010 and September 2010, at numerous locations under the purview of the National Nuclear Security Administration (NNSA), Under Secretary of Energy, and Under Secretary for Science. 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 our objective, we:

- Reviewed Federal statutes and Department directives pertaining to information and cyber security such as the *Federal Information Security Management Act of 2002*, Office of Management and Budget (OMB) Circular A-130 (Appendix III), and DOE Order 205.1A, *Department of Energy Cyber Security Management*;

- Reviewed applicable standards and guidance issued by OMB and the National Institute of Standards and Technology (NIST) for the planning and management of system and information security such as OMB Memorandum 10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*; and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information System*;

- Obtained and analyzed documentation from Department programs and certain sites pertaining to the planning, development, and management of cyber

security related functions such as program cyber security plans, plans of action and milestones, and budget information; and,

- Held discussions with officials from the Department and NNSA.

We conducted this evaluation in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. 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 its information and cyber security program. 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 solely rely on computer-processed data to satisfy our objective. 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 and NNSA waived an exit conference.

RELATED REPORTS

Office of Inspector General Reports

- *Internal Controls over Computer Hard Drives at the Oak Ridge National Laboratory* (INS-O-10-03, August 2010). The Oak Ridge National Laboratory's (ORNL) controls over the tracking of hard drives, which may contain sensitive unclassified information, were inadequate to prevent the unauthorized dissemination of sensitive unclassified information. Specifically, it had not implemented controls to encrypt, or track and control, hard drives that may contain sensitive unclassified information.

- *Management Controls over the Development and Implementation of the Office of Energy Efficiency and Renewable Energy's Performance and Accountability for Grants in Energy (PAGE) System* (OAS-RA-10-14, July 2010). The PAGE system was placed into operation before the required cyber security planning and testing was completed. This lack of planning and testing placed the PAGE system and the network on which it resided at increased risk that the confidentiality, integrity, and availability of the Department of Energy's (Department) information systems and data could be compromised.

- *The Department's WinSAGA System for Energy Grants Management Under the Recovery Act* (OAS-RA-10-05, March 2010). System security planning documentation and control testing was incomplete and inconsistent. For example, the information contained in the system security plan was not representative of the entire computing environment. Also, a significant portion of the required security controls were excluded from testing. This exposed the system and data to a higher than necessary level of risk of compromise, loss, modification, and non-availability.

- *Management Challenges at the Department of Energy* (DOE/IG-0832, December 2009). Based on the work performed during Fiscal Year (FY) 2009 and other risk assessment tools, the Office of Inspector General identified six areas, including cyber security, remained as management challenges for FY 2010.

- *The Office of Science's Management of Information Technology Resources* (DOE/IG-0831, November 2009). For non-scientific computing environments, all seven of the field sites reviewed (two Federal, five contractor) had implemented security configurations that were less stringent than those included in the Federal Desktop Core Configuration (FDCC). This configuration was designed by the National Institute of Standards and Technology to ensure that Federal information systems had implemented a specific baseline of security controls, and its use was mandated by the Office of Management and Budget. Although Office of Science Headquarters had documented its rationale for deviating from the FDCC configuration, none of the seven field sites had identified and documented their deviations, as required.

- *The Department's Unclassified Cyber Security Program - 2009* (DOE/IG-0828, October 2009). Opportunities were identified for improvements in areas such as security planning and testing, systems inventory, access controls, and configuration

management. In particular, a number of findings at sites managed by the National Nuclear Security Administration were issued. We also identified weaknesses across various Department program elements.

- *Protection of the Department of Energy's Unclassified Sensitive Electronic Information* (DOE/IG-0818, August 2009). Opportunities existed 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 threats; and, were still working to complete required Privacy Impact Assessments.

- *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.

Government Accountability Office Report

- *Government-wide Guidance Needed to Assist Agencies in Implementing Cloud Computing* (GAO-10-855T, July 2010)

- *Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats* (GAO-10-834T, June 2010)

- *Key Challenges Need to Be Addressed to Improve Research and Development* (GAO-10-466, June 2010)

- *Federal Guidance Needed to Address Control issues with Implementing Cloud Computing* (GAO-10-513, May 2010)

- *Concerted Response Needed to Resolve Persistent Weaknesses* (GAO-10-536T, March 2010)

- *Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience* (GAO-10-296, March 2010)

- *Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies* (GAO-10-237, March 2010)

- *Continued Efforts are Needed to Protect Information Systems for Evolving Threats* (GAO-10-230T, November 2009)

- *Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network* (GAO-10-28, October 2009)

- *Leadership Needed to Strengthen Agency Planning Effort to Protect Federal Cyber Assets* (GAO-10-148, October 2009)

- *Current Cyber Sector-Specific Planning Approach Needs Reassessment* (GAO-09-969, September 2009)

- *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 2009)

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

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

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

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

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

Department of Energy
Washington, DC 20585

October 12, 2010

MEMORANDUM FOR RICKEY R. HASS
DEPUTY INSPECTOR GENERAL
FOR AUDIT SERVICES
OFFICE OF INSPECTOR GENERAL

FROM: WILLIAM T. TURNBULL
CHIEF INFORMATION OFFICER (ACTING)

SUBJECT: Inspector General's Draft Report on Evaluation Report on *The Department's Unclassified Cyber Security Program – 2010* (A10TG016)

The Department of Energy's (DOE) Office of the Chief Information Officer (OCIO) appreciates the opportunity to comment on this draft report and the Office of the Inspector General's (IG) recognition of the Department's progress over the past year in addressing weaknesses and enhancing its unclassified cyber security program.

At the same time, the OCIO disagrees, in part, with the IG's characterization of the scope, severity, and cause of the issues presented in the report. Specifically:

- The Department's Cyber Security Governance Council has unanimously approved the recommendation of its advisory bodies to implement a mission centric, risk-based approach in the management of the Department's cyber security program. This approach emphasizes the authority and responsibility of the Under Secretaries and site management to make risk-based decisions in the implementation of cyber security. Cyber security controls are applied using national standards (i.e., National Institute of Standards and Technology (NIST)) and a graded protection approach based on management's determination and acceptance of risk. The goal with this approach is not only to protect the mission, but to enable it.
- Data gathered from vulnerability scanning is not in and of itself sufficient for informing management decisions. These data are only partial indicators that must be evaluated in a broader context. Absent additional data and further investigation, findings should not be equated with risk. Management leverages vulnerability scan data and other inputs, along with risk assessments, to build a decision matrix. Management must appropriately prioritize actions in the context of mission assurance and operational imperatives.
- The Department's information systems are enormous in number and varied in scope. The sites the IG visited this year alone have perhaps hundreds of thousands of devices under their care. Finding a fractional percentage of misconfigured devices at these sites does not inherently suggest widespread weaknesses of control, contrary to the report's implications. Additionally, the

report does not indicate if the misconfigured machines or policy deficiencies are within a site's acceptable risk envelope, nor does the assessment account for compensating controls or mitigating elements in sites' layered defenses. While identifying potential issues is important, the impact should not be overstated against the backdrop of a wide ranging and complex infrastructure.

- The Department's systems are all protected by defense in depth approaches. The finding of a particular technical misconfiguration should not be construed as representing substantial risk to DOE's systems. Further, substantive risks to systems at one site should not be assumed to pose similar risks to other sites. We are concerned that the report conveys an inaccurate view of real risk to DOE's information resources.
- The Department's information systems are managed in a federated way, in large part by its M&O contractors. The IG's characterization of problems "recurring" across the Department belies the complexity of the operations and unique operating relationships across DOE. Securing systems is complex and variable, and while the Department undertakes significant effort to prevent and respond to security findings, it is expected that there will continue to be variation and normal error across the diversity of the Department's operations.
- We share the IG's goal to improve our cyber security programs and better protect the missions of DOE. To better facilitate the process for achieving this goal, we request that the IG provide copies of its working papers, including documentation of methodology and statistical methods, whenever it is submitting draft reports for management response/reaction.

Finally, we are concerned that the IG mischaracterizes the way in which a substantial amount of its business is conducted: through M&O contractors. For example, the IG is concerned that POA&Ms do not have budget numbers associated with them, and that this prevents effective prioritization; however, this belies the essential character of the organizational relationship where M&Os are responsible for allocating funding for security and other priorities utilizing risk management principles. Similarly, the IG cites lack of oversight as a driver for these concerns in several areas; however, the Department does not expect local oversight to be responsible for finding each misconfiguration or error – in fact to do so would undermine the notion of performance based contracting. Instead, oversight can and should be evaluate the M&O's success in effectively managing risk.

In conclusion, we are appreciative of the IG's efforts in this area, but concerned that the implications regarding critical elements in this report may be misinterpreted and lead to the erroneous conclusion that the Department and its contractors are not exercising appropriate stewardship over its information resources.

The DOE Office of the CIO concurs, for the most part, on the report's recommendations, specifically:

Recommendation 1: *Correct, through the implementation of appropriate controls, the weaknesses identified within this report.*

Concur. The findings identified in this report will be addressed in accordance with the Department's risk management approach.

Recommendation 2: *Ensure that policies and procedures are developed, as needed, and are effectively implemented to secure systems and applications.*

Concur. The Department's Cyber Security Governance Council and its advisory groups have been reviewing all Departmental cyber security policies and, as appropriate, revising them to ensure cyber security is governed using a risk management approach. The Department has completed a draft Directive, *Department of Energy Cyber Security Management (DOE Order 205.1B)* and expects to publish the revised directive in the near future.

Recommendation 3: *Implement an adequate compliance monitoring program, such as the use of periodic evaluations by Headquarters' management, to ensure the effectiveness of the cyber security program performance.*

Concur. The Department's risk management approach includes a revised oversight model that focuses on program performance and addresses the elements of this recommendation.

Recommendation 4: *Ensure that POA&Ms are fully developed and utilized to track, prioritize, and enable remediation of all known cyber security weaknesses.*

Concur in part. The OCIO, in coordination with the Cyber Security Governance Council, is evaluating which changes need to be made to improve the process for tracking and closing deficiencies in accordance with the Department's risk management approach and contractor assurance model.

If you have further questions, please contact Mr. Collis Woods, Acting Associate CIO for Cyber Security, at 202-586-9805.

National Nuclear Security Administration

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

OCT 18 2010

MEMORANDUM FOR: Rickey R. Hass
Deputy Inspector General
for Audit Services
Office of Inspector General

FROM: Gerald L. Talbot, Jr.
Associate Administrator
for Management and Administration

SUBJECT: Comments to the IG's Draft Report on FISMA – 2010;
Project No. A10TG016; IDRMS No. 2010-00405

The National Nuclear Security Administration (NNSA) appreciates the opportunity to provide comments to the Inspector General's (IG) report, *The Department's Unclassified Cyber Security Program – 2010*. I understand that this audit was performed to determine whether the Department's unclassified cyber security program adequately protected its information and systems.

As an Agency, it would be beneficial if the IG would issue a separate report to NNSA that specifically reviews our 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 appreciates the IG's recognition of the progress that has been made over the past year in addressing weaknesses and enhancing the unclassified Cyber Security Program. NNSA implements a flexible, comprehensive, and risk-based cyber security program that (a) adequately protects the NNSA information and information assets; (b) is predicated on public laws, Executive Orders, and national standards; and (c) results in a policy-driven cyber security architecture. This robust security framework is aligned with the NNSA enterprise architecture, providing a programmatic framework and methodology that integrates all of the components of a comprehensive cyber security program to fully support the NNSA mission.

The NNSA OCIO is committed to fully addressing the recommendations outlined by the IG in the report. This commitment includes the development of corrective action plans to address each of the recommendations and follow-up site assessment visits by the OCIO assessment team to ensure corrective actions are implemented.

At the same time, we have concerns about the IG's characterization of the scope, severity, and cause of the issues presented here. Specifically:

- The information systems within the Nuclear Security Enterprise (NSE) are enormous and vary in scope. The sites the IG visited this year alone have over 50,000 computing devices, consisting of laptops, desktops and servers under their purview. Therefore, although the IG's audit identified a small number of systems that were determined to be misconfigured or had policy deficiencies, it is important to recognize that each site is operating within its risk acceptance model. While the IG's audit program's role in identifying deficiencies is an important element of the agency's overall internal control scheme (and, as noted above, NNSA will take prompt action to address issues/deficiencies that are identified) it is also important not to overstate the impact of a few instances of misconfigured systems or policy deficiencies which are within the site's risk acceptable envelope.

- All NNSA systems are protected by distinctive, layered, and defense in-depth approaches. Therefore, the finding of a particular technical misconfiguration, does not necessarily translate to substantive or systemic risk to NNSA's systems. Furthermore, substantive risks to systems at one site almost certainly present no or extremely limited risks to other sites. Each site has its own security architecture, including firewalls, intrusion detection, antivirus, network monitoring, and physical security that operate independent of the other sites. We are concerned that a casual reader of this report might not fully understand that the findings, while important, do not necessarily represent demonstrated risks. Nonetheless, we will use the work of the IG here as a source of lessons learned for other sites within the NSE.

- NNSA's information systems are managed by Management and Operating (M&O) contractors with Federal oversight. The IG's characterization of "recurring" problems across the NSE inaccurately reflects the complexity of the operations and unique operating relationships across NNSA as described above. Risks to the most sensitive systems and information are not acceptable. NNSA sites recognize different levels of risk and implement strategies to mitigate those risks based upon sound risk management principles. It is important that when describing a deficiency, the description adequately characterize the impact of the potential exposure as it relates to that specific workstation, server, network and enterprise.

Finally, we are concerned that the IG does not accurately characterize the way in which a substantial amount of its business is conducted through M&O contractors. For example, the IG is concerned that plans of actions and milestones (POA&Ms) do not have budget figures associated with them, and concludes that this would prevent prioritization. The report also cites lack of oversight as a driver for these concerns in several areas. However, NNSA does not expect local oversight to be responsible for finding all site deficiencies but relies on performance-based contracting, risk management, and periodic verification and validation to provide the reasonable assurance of good performance. Therefore, we believe the focus should be on Federal oversight of the M&O's ability to effectively manage risks, and thereby, prevent security incidents.

In conclusion, we appreciate the IG's efforts in this area. However, we are concerned the casual reader of this report may lack the context, technical cyber security knowledge and risk management expertise required to draw accurate and meaningful conclusions regarding the Department's stewardship of our unclassified information technology assets.

NNSA agrees with the report's recommendations. Below are the responses to those recommendations. Please note that actions agreed upon by our concurrence are an ongoing process. Consequently, a specific date for completion of these recommendations cannot be provided at this time.

Recommendation 1: *Correct, through the implementation of appropriate controls, the weaknesses identified within this report.*

The NNSA's Office of Chief Information Officer (OCIO) will work in concert with the NNSA Site Offices and the M&O contractors to ensure that specific control weaknesses are addressed in a manner that will is consistent with the risk management principles and missions in question.

Recommendation 2: *Ensure that policies and procedures are developed, as needed, and are effectively implemented to secure systems and applications.*

During the past year the OCIO has been collaborating and coordinating with the NNSA Site Office and M&O contractor IT and cyber security personnel to develop comprehensive policies and procedures that adhere to national standards (NIST, FIPS and CNSS). This will ensure this effective implementation of secure systems, applications and networks across the Nuclear Security Enterprise (NSE). The implementation of these policies and procedures will provide the NSE with the ability to ensure that enterprise and local risk management approaches are adopted complex-wide.

Recommendation 3: *Implement an adequate compliance monitoring program, such as the use of periodic evaluations by headquarters management, to ensure the effectiveness of cyber security program performance.*

The risk management approach and implementation of a contractor assurance model is intended to specifically address the elements of this recommendation. However, the use of Headquarters management in this area, in lieu of Site Office and M&O staff, may undermine the broader efforts at assurance and oversight reform within NNSA. Actions in this area will be consistent with the direction set by the Administrator and Deputy Administrator for transforming oversight activities within NNSA.

4

Recommendation 4: *Ensure that POA&Ms are fully developed and utilized to track, prioritize, and enable remediation of all known cyber security weaknesses.*

The NNSA OCIO coordinates with the NNSA's Program and Staff Offices which provide quarterly POA&M updates. However, the use of these as a management tool by the M&O contractors is questionable since these are a federal system function, not a local site function. The OCIO is evaluating what changes need to be made in the POA&M program to better align its contracting model with the need to track deficiencies.

If you have any questions concerning this response, please contact JoAnne Parker, Director, Office of Internal Controls, at 202-586-1913.

cc: James Cavanagh, Acting Chief Information Officer
Wayne Jones, Deputy Chief Information Officer for Cyber Security

IG Report No. DOE/IG-0843

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.

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.