



U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Evaluation Report

The Department's Unclassified
Cyber Security Program – 2011




Department of Energy
Washington, DC 20585

October 20, 2011

MEMORANDUM FOR THE SECRETARY

FROM:


Gregory H. Friedman
Inspector General

SUBJECT:

INFORMATION: Evaluation Report on "The Department's Unclassified Cyber Security Program – 2011"

INTRODUCTION AND OBJECTIVE

The Department of Energy's numerous information systems are routinely threatened with sophisticated cyber attacks. According to the Office of Management and Budget and the Department of Homeland Security's U.S. Computer Emergency Readiness Team, cyber attacks against Federal agencies' websites and networks increased almost 40 percent last year. Attackers continued to exploit vulnerabilities in applications and products. To mitigate the risks associated with cyber security threats, the Department expended significant resources in Fiscal Year (FY) 2011 on cyber security measures designed to secure its systems and information that support various program operations to advance energy and national security, scientific discovery and innovation, and environmental responsibility.

The Federal Information Security Management Act of 2002 (FISMA) established requirements for all Federal agencies to develop and implement agency-wide information security programs. FISMA also directed Federal agencies to provide appropriate levels of security for the information and systems that support the operations and assets of the agency, including those managed by another agency or contractors. As required by FISMA, the Office of Inspector General conducted an independent evaluation to determine whether the Department's unclassified cyber security program adequately protected its data and information systems. This memorandum and the attached report document the results of our evaluation for FY 2011.

RESULTS OF EVALUATION

The Department had taken steps over the past year to address previously identified cyber security weaknesses and enhance its unclassified cyber security program. While these were positive steps, additional action is needed to further strengthen the Department's unclassified cyber security program and help address threats to its information and systems. For example, our FY 2011 evaluation disclosed that corrective actions had been completed for only 11 of the 35 cyber security weaknesses identified in our FY 2010 review. In addition, we identified numerous weaknesses in the areas of access controls, vulnerability management, web application integrity, contingency planning, change control management, and cyber security training. While many of the same or similar issues had been noted in prior FISMA reports, the number of weaknesses identified represented a 60 percent increase over our FY 2010 review. Specifically:

- At 11 locations, including Headquarters, we identified 18 deficiencies related to access controls, such as failure to perform periodic management reviews of user accounts,

inadequate management of user access privileges, default or weak usernames and passwords, lack of segregation of duties, and lack of logging and monitoring of user activity;

- We identified 21 weaknesses related to vulnerability management at 15 locations. Specifically, we found desktops and network systems and devices running applications without current security patches for known vulnerabilities – situations that could allow unauthorized access to system resources;
- At 10 locations, we identified 14 weaknesses in at least 32 different web applications used to support functions such as procurement and safety. These vulnerabilities could be exploited by attackers to deliberately or inadvertently manipulate network systems;
- One of the sites we reviewed had not developed a business continuity/disaster recovery plan or an overall business impact analysis – key elements designed to correlate specific system components with the services that are provided and characterize the consequences of a disruption to the system;
- Change control management weaknesses were also observed at several locations. For example, we determined that although one site had developed a Cyber Security Configuration Management Procedure that required the system change control process to include testing or modeling the impact of changes to the current system, it had not properly maintained application change test plans and results; and,
- Finally, we found that one site had not fully implemented an annual cyber security refresher training program designed to provide basic security awareness training to all users.

The weaknesses identified occurred, in part, because Departmental elements had not ensured that cyber security requirements included all necessary elements and were properly implemented. Program elements also did not always utilize effective performance monitoring activities to ensure that appropriate security controls were in place. Without improvements to its unclassified cyber security program, such as consistent risk management practices and adopting processes to ensure security controls are appropriately developed, implemented and monitored, there is an increased risk of compromise and/or loss, modification, and non-availability of the Department's systems and information. As observed in the recent cyber attacks at four sites, exploitation of vulnerabilities can cause significant disruption to operations and/or increase the risk of modification or destruction of sensitive data or programs.

As the number of cyber security threats increases, including attacks from both domestic and international sources, it has become increasingly important that the Department intensify efforts to safeguard its systems and the information they contain. During the past year, the Department had taken action to update its cyber security policy, and the National Nuclear Security Administration (NNSA) had reestablished periodic site-level cyber security reviews. However, given the increased number of vulnerabilities discovered this year, it is clear that continued

vigilance is necessary. In this regard, we made several recommendations to help the Department strengthen its unclassified cyber security program for protecting its systems and data from the threat of compromise, loss or modification.

Due to security considerations, information on specific vulnerabilities and locations has been omitted from this report. Site and program officials were provided with detailed information regarding respective vulnerabilities identified and, in many instances, corrective actions were initiated.

MANAGEMENT REACTION

Management concurred with the report's recommendations and disclosed that it had initiated or already completed actions to address issues identified in our report. NNSA officials expressed concern with our characterization of the scope, severity, and cause of the issues presented in our report. NNSA also criticized our evaluation approach, asserting that it focused strictly on a compliance checklist approach that did not adequately consider current Federal policies relating to risk-based, cost effectiveness approaches to cyber security.

We take specific exception to NNSA's characterization of our work. Our findings were based on targeted tests of systems using a wide variety of recognized tools and methods. As a matter of course, we specifically considered risk acceptance and compensating controls. In addition, our work was based on Federal cyber security requirements that were relevant to the period of evaluation and provided for consideration of risk and cost effectiveness. Finally, the results of the evaluation cannot be directly projectable to the entire universe of Department systems and we do not attempt to do so. However, we believe that it would be prudent to ensure that the vulnerabilities that we have identified are considered throughout the complex in a cost effective way. Management's comments and our response are summarized and more fully discussed in the body of our report. Management's formal comments are included in their entirety in Appendix 3.

Attachment

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

EVALUATION REPORT ON THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM - 2011

TABLE OF CONTENTS

The Department's Unclassified Cyber Security Program

Details of Finding	1
Recommendations and Comments.....	8

Appendices

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

The Department's Unclassified Cyber Security Program – 2011

Program Improvements

The Department of Energy (Department) had taken steps to address previously identified cyber security weaknesses and enhance its unclassified cyber security program. We found that corrective actions had been taken to resolve 11 of 35 weaknesses identified during our Fiscal Year (FY) 2010 evaluation of *The Department's Unclassified Cyber Security Program - 2010* ([DOE/IG-0843](#), October 2010) related to configuration and vulnerability management, access controls, system integrity, performance monitoring, and oversight. Also, the Department had made additional changes to its unclassified cyber security program in response to the growing cyber security threat. Specifically:

- The National Nuclear Security Administration (NNSA) corrected a previously identified weakness from our FY 2007 review by reestablishing periodic site evaluations to review the effectiveness of Federal field site offices in carrying out their responsibilities for proper implementation of Federal cyber security requirements by field organizations and facility contractors. At the time of our review, several unclassified assessments had been completed; and,
- The Department issued Order 205.1B, *Department of Energy Cyber Security Program*, in May 2011. The key elements of the revised Directive include continuous monitoring and assessment of the risk management process, and required that Federal oversight be conducted through assurance systems that monitor the risk evaluation and protection processes at each level in the organization.

Security Controls and Risk Management

Although the Department made progress addressing previously identified conditions, we continued to find weaknesses similar in type and risk level to those identified during our FY 2010 review. Our review of the Under Secretary for Nuclear Security, Under Secretary for Science, and Under Secretary of Energy organizations identified various control weaknesses related to access controls, vulnerability management, integrity of web applications, contingency planning, change control management, and cyber security training. Based on the results of our work, we noted that the number of weaknesses increased significantly for the second year in a row, including a 60 percent increase in the number of weaknesses since last year.

Based on testing conducted at 25 locations, including Headquarters, there were 32 new weaknesses identified and 24 weaknesses remained from the prior year's review. In a number of instances, site officials took action to correct certain weaknesses shortly after we identified them. The weaknesses we discovered are detailed in the remainder of our report.

Access Controls

Although the Department corrected four of nine previously identified access control weaknesses, it continued to experience vulnerabilities in this area. 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. We identified 18 access control deficiencies at 11 locations reviewed. In particular:

- We identified 12 account management weaknesses at 8 locations, including failure to perform periodic management reviews of user accounts and adequately manage user access privileges. Access privileges that were not adequately managed included account establishment, modification, review, disablement, and removal. While officials at one site had conducted a review, they had not removed responsibilities for nine users that no longer required access to perform their job function;
- Internal vulnerabilities involving weak access controls in network services related to default or weak username and passwords were observed at four sites reviewed. At one location, a network server system was configured to accept connections from another system without the use of authentication or similar access controls, which would allow remote control of the affected system. At another site, we found eight network services and/or devices with password management weaknesses. Furthermore, we noted weaknesses at one site that could allow an attacker to exploit this vulnerability to obtain access to the operating system supporting the production database server;
- We identified three locations with segregation of duties issues. Specifically, system administrators used their privileged accounts to inappropriately perform both

privileged and non-privileged functions. Segregation of duties is a critical control that ensures the separation of the functions of authorizing, processing, recording, and reviewing input data; and,

- One site did not log and monitor its information system activities. Absent effective audit and accountability practices, including information system auditing, logging, and monitoring, the risk of malicious or unauthorized access to the unclassified network, systems and related applications may be increased.

Vulnerability Management

Despite corrective actions initiated to resolve vulnerability management issues identified in our prior evaluation, we continued to find weaknesses similar in type and risk level. In total, we identified 21 weaknesses related to vulnerability management at 15 locations. The weaknesses consisted of varying degrees of vulnerable applications, desktops, and network systems missing security updates and/or patches for known vulnerabilities. As weaknesses were identified, we considered the implementation of compensating controls, as appropriate. Specifically:

- During the FY 2010 review, we identified 13 vulnerability and patch management internal weaknesses on desktop applications and 6 internal weaknesses on network systems and devices. Although four of six vulnerabilities for network systems and devices were addressed this year, none of the desktop vulnerabilities were corrected. In addition, we identified new desktop weaknesses at two sites and network vulnerabilities at three sites not identified during our prior year evaluation;
- Our review identified that 3,014 of 6,512 (46 percent) desktop systems tested were running operating systems and/or client applications without current security patches for known vulnerabilities. These applications were missing security patches for known vulnerabilities that had been released more than 3 months prior to our testing; and,
- We identified 52 network systems and devices that were running operating systems and application support platforms without current security patches and/or

security configurations for known vulnerabilities that were released more than 30 days prior to testing. We also identified 20 network server systems running operating system versions that were no longer supported by the vendor.

Some of the identified vulnerabilities affected systems and other servers hosting financial and non-financial applications that could have permitted individuals to gain administrator level access. Although some sites provided risk management plans and mitigating controls for the weaknesses identified, many of the programs' and sites' risk acceptance was not specific, accurate, and complete. We also found that, in many cases, sites had not accepted the risk of certain vulnerabilities until after we discovered them. In addition, while certain controls existed, they were not always adequate to mitigate risk or prevent a hacker from potentially exploiting the applications.

Integrity of Web Applications

The Department's internal controls over the integrity of web applications did not always ensure that input data was validated and the web application was secure against unauthorized access and modification of data. Specifically, our performance testing found at least 32 web applications, used to support functions such as procurement and safety, did not perform validation procedures. Such procedures ensure that changes made to information and programs are only allowed in a specified and authorized manner and that the system's operation is not impaired by deliberate or inadvertent unauthorized manipulation, such as through software flaws and malicious code. However, we found that:

- Ten locations were operating web applications that contained functional design flaws and did not properly validate input data. At one of the sites, the application included a password test function that could allow an attacker to determine or modify the password for any valid user account; and,
- One location maintained a web application that did not protect accounts from brute force attacks against the "change password" function. Such attacks could allow a hacker to potentially change a user's password and gain access to the application.

Web applications that do not properly protect access control functions are at risk of malicious attacks that could result in unauthorized access to application functionality and sensitive data stored in the application.

Contingency Planning

Our testing found that one site had weaknesses related to contingency planning. Although the contingency planning processes at the site had improved, management had not developed a business continuity/disaster recovery plan to define emergency and restoration requirements for its information systems. In addition, we noted that the site had not developed an overall business impact analysis to characterize the consequences of a disruption to the system components. Absent effective contingency planning and a disaster recovery program, including formally documented business continuity/disaster recovery plans and a business impact analysis, these weaknesses may increase the risk of loss of critical information and data in certain types of disasters.

Change Control Management

We identified change control weaknesses at several locations. Specifically, we determined that although one site had developed procedures that required testing or modeling the impact of changes being made to a system, it had not properly maintained application change test plans and results. In addition, our ongoing audit of the *Department's Configuration Management of Non-Financial Systems* identified that system and application changes did not always follow recommended procedures, including approval, testing, and documenting the risks associated with potential changes. Controls of this type are an integral component of a strong security policy and help to ensure that computer applications and systems are consistently configured with minimum security standards to prevent and protect against unauthorized modifications.

Cyber Security Training Program

We noted that one site had weaknesses related to its cyber security training program. Although it had made improvements in developing a security awareness training program since the prior year review, including initial and annual refresher security awareness training, the site had not fully implemented an annual cyber security refresher training program. Within a year's time, only 35 of 1,980 users had

completed annual refresher security awareness training. Effective security awareness training can be particularly useful in preventing certain types of activities, such as successful phishing attacks.

Implementation of Requirements and Performance Monitoring

The weaknesses identified occurred, in part, because Departmental elements had not ensured that cyber security requirements included all necessary elements and were properly implemented. In addition, Department programs and sites did not always utilize effective performance monitoring activities to ensure that appropriate security controls were in place.

Procedures and Processes

The cyber security control weaknesses identified were due, in part, to inadequate development and implementation of security control processes. In particular, programs and sites developed policies and procedures that did not always satisfy Federal or Departmental security requirements. For instance, we noted that policies at certain programs and sites were not aligned with Federal requirements related to access controls and vulnerability/configuration management. At one site, officials commented that they were not required to follow Office of Management and Budget (OMB) guidance since it was not documented in their contract or the Contractor Requirements Document.

Furthermore, even when policies and procedures were in place, they were not always implemented. Specifically, many of the programs and sites reviewed had not followed site-level patch management policies and procedures to ensure that security updates were consistently applied in a timely manner. In addition, many sites had established access control processes that were not completely effective. For example, although one site had established a process for disabling accounts that were inactive for more than 60 days and deleting accounts that were inactive for more than 12 months, the location had not yet fully implemented the process. Another site did not follow established access control processes for retaining all approved enrollment forms for granting information system access to new users. In addition, one site had not fully implemented requirements related to logging and monitoring its information systems activities.

Performance Monitoring

As noted in prior years, steps had not been taken to ensure that performance monitoring activities were effective. For example, we found that many sites had not implemented an effective process to ensure that security patch management processes for desktops, network devices, and applications were working as designed. In addition, many of the web application vulnerabilities we identified occurred because programs and sites did not implement effective monitoring processes to ensure that controls were in place to identify and prevent application integrity issues. As the Department moves closer to relying on contractor assurance processes to monitor the effectiveness of programs, it is essential that adequate performance monitoring mechanisms are in place.

In addition, Plans of Action & Milestones (POA&Ms) were not always effectively used to report, prioritize, and track cyber security weaknesses through remediation. Specifically:

- Many of the sites reviewed had tracked weaknesses at a local level; however, similar to last year's evaluation, we found that 15 of 35 cyber security deficiencies identified during our FY 2010 evaluation were not reported in the Department's POA&Ms maintained by the Office of the Chief Information Officer (OCIO), as required by OMB. In addition, POA&Ms did not contain all cyber security weaknesses identified in numerous security related Office of Inspector General reports;
- Our evaluation identified approximately 45 percent of open milestones captured in the POA&Ms were beyond their original projected remediation date. For instance, we noted that 103 open milestones were at least 1 year beyond their estimated remediation date; and,
- Although required by the Department and OMB, POA&Ms were not requested by or submitted to the OCIO for the first and third quarters of FY 2011, which limited the OCIO's ability to identify areas of concern and review the progress of cyber security weakness remediation.

As noted by the National Institute of Standards and Technology (NIST), 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 unclassified cyber security program, such as consistent risk management practices and adopting processes to ensure security controls are fully developed and implemented, there is an increased risk of compromise and/or loss, modification, and non-availability of the Department's systems and information. Although many sites had implemented certain compensating controls to mitigate the risk associated with vulnerabilities, our testing revealed that malicious individuals could execute attacks against the vulnerable systems, applications, and user desktops by using sophisticated methods.

As noted by recent successful attacks at four Department locations, exploitation of vulnerabilities can cause significant disruption to operations and/or increases the risk of modification or destruction of sensitive data or programs, and possible theft or improper disclosure of confidential information. In addition, recovery efforts for these attacks can be very costly. For example, the estimated cost to the Department for the recent cyber attacks at three of the four sites was over \$2 million. Therefore, continued vigilance is necessary due to the recent Department incidents and increased cyber attacks by both domestic and international sources.

RECOMMENDATIONS

In light of the issues identified in our report, it is essential that the Department effectively implement its new Order 205.1B, *Department of Energy Cyber Security Program*, to aid in the continuous monitoring and assessment of the risk management process. To help ensure these processes are fully implemented and to address the weaknesses identified in this report, we recommend that the Under Secretary for Nuclear Security, 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 implemented in accordance with Federal and Department requirements to adequately secure systems and applications;

-
3. Ensure that effective performance monitoring practices are implemented to assess overall performance for protecting information technology resources; and,
 4. Ensure that POA&Ms are developed and used to prioritize and track remediation of all cyber security weaknesses requiring corrective actions.

**MANAGEMENT
REACTION AND
AUDITOR COMMENTS**

Department and NNSA management concurred with the report's recommendations and stated that it had taken or initiated corrective actions to address each of the recommendations. For instance, Department management noted that Order 205.1B, *Department of Energy Cyber Security Program*, required senior management organizations to develop and implement procedures and processes for securing information, systems and applications. In addition, management disclosed that it was working towards the use of a centralized repository for POA&M reporting to improve accuracy and ease of reporting. NNSA management commented that its 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.

While NNSA concurred with our recommendations, it disagreed with the characterization of the scope, severity, and cause of the issues presented in our report. We have summarized NNSA management's comments and provided our response for each. Management's comments are included in their entirety in Appendix 3.

NNSA management commented that finding a relatively small number of misconfigured devices at the sites reviewed did not inherently suggest widespread weaknesses of control and that the fractional percentages of misconfigured devices identified were isolated issues at the system-level and not across the Nuclear Security Enterprise. 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.

We agree that the results of our vulnerability testing cannot be projected across the Department and, as such, did not attempt to do so in our report. However, given that the vulnerabilities identified within NNSA spanned desktops, applications, and network devices, we do not believe that our findings are necessarily isolated incidents. As noted in the report, our test

work revealed that the weaknesses, if exploited, could have permitted a malicious user to compromise systems or data. As part of our test work, we fully considered site-level risk assessments and compensating controls. As such, many of the vulnerabilities initially identified during our evaluation were not included in this report based on our discussions with site officials related to their acceptance of risk and related compensating controls. In many cases, sites were unaware of the vulnerabilities we identified prior to our testing.

NNSA management commented that although previous efforts to implement security controls consistently throughout the Federal government focused on compliance with specific controls and technologies, NIST recently updated policies and guidance supporting a unified risk-based information security framework to implement cost-effective security controls. Management asserted that audits continue to be based upon system compliance checklists and not according to current cyber security methodologies that target the strength of layered defense strategies that will effectively mitigate some of the risks to an acceptable level, as well as significantly reduce the cost and burden of implementation and maintenance of certain security controls at the system-level.

The Federal Information Security Management Act of 2002 requires us to evaluate the Department's security posture against Federal standards, including the consideration of risk acceptance practices and compensating controls. Our test work was not based on compliance checklists, but rather used a wide range of tools to evaluate the effectiveness of security controls. For instance, our vulnerability testing included both internal and external testing that utilized tools readily available to hackers and other malicious individuals. In addition, our testing methodology is regularly evaluated and updated to keep pace with evolving cyber security threats.

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 2011 and October 2011, at numerous locations under the purview of the National Nuclear Security Administration (NNSA), Acting 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 Enforcement and Oversight performed a separate evaluation of the Department's information security program for national security systems.

METHODOLOGY To accomplish our objective, we:

- Reviewed Federal regulations, Departmental 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 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 Systems and Organizations*;
- 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 review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings 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 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

- *Department's Management of Cloud Computing Services* ([OAS-RA-L-11-06](#), April 2011). We noted several opportunities for improvement in the Department of Energy's (Department) cloud computing initiative and that certain areas related to management of the Magellan Project could be enhanced. Specifically, the Department had not yet prepared policies and procedures governing security and other risks and had not established coordination requirements among sites to prevent duplication or other problems with cloud deployment and problems existed with resource disposition plans and American Recovery and Reinvestment Act of 2009-related job reporting for the Magellan Project.
- *Management Challenges at the Department of Energy* ([DOE/IG-0844](#), November 2010). Based on the work performed during Fiscal Year (FY) 2010 and other risk assessment tools, the Office of Inspector General identified seven areas, including cyber security and safeguards and security, that remained as management challenges for FY 2011.
- *The Department's Unclassified Cyber Security Program - 2010* ([DOE/IG-0843](#), October 2010). Opportunities were identified for improvements in areas such as access controls, configuration and vulnerability management, web application integrity, and security planning and testing. In particular, Departmental elements had not always ensured that cyber security requirements were effectively implemented. In addition, the Department had not adequately monitored cyber security performance.
- *Internal Controls over Computer Hard Drives at the Oak Ridge National Laboratory* ([INS-O-10-03](#), August 2010). The Oak Ridge National Laboratory's 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 System* ([OAS-RA-10-14](#), July 2010). The Performance and Accountability for Grants in Energy (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's information systems and data could be compromised.
- *Management Controls over the Department's WinSAGA System for Energy Grants Management Under the Recovery Act* ([OAS-RA-10-05](#), March 2010). System

Appendix 2 (continued)

- 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.
- *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.
 - *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 Reports

- *Information Security: Government-wide Guidance Needed to Assist Agencies in Implementing Cloud Computing* ([GAO-10-855T](#), July 2010)
- *Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats* ([GAO-10-834T](#), June 2010)
- *Cybersecurity: Key Challenges Need to Be Addressed to Improve Research and Development* ([GAO-10-466](#), June 2010)

Appendix 2 (continued)

- *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing* ([GAO-10-513](#), May 2010)
- *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience* ([GAO-10-296](#), March 2010)
- *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies* ([GAO-10-237](#), March 2010)
- *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats* ([GAO-10-230T](#), November 2009)
- *Information Security: Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network* ([GAO-10-28](#), October 2009)
- *Critical Infrastructure Protection: OMB Leadership Needed to Strengthen Agency Planning Efforts to Protect Federal Cyber Assets* ([GAO-10-148](#), October 2009)
- *Critical Infrastructure Protection: 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)

Appendix 2 (continued)

- *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)



Department of Energy
Washington, DC 20585

October 12, 2011

MEMORANDUM FOR: Mr. Rickey R. Hass
Office of Inspector General

FROM: Michael W. Locatis, III *MW Locatis*
Chief Information Office

SUBJECT: Inspector General's Draft Evaluation Report on the
"Department's Unclassified Cyber Security Program –
2011"

The Department of Energy's (DOE) Office of the Chief Information Officer (OCIO) appreciates the opportunity to comment on the Office of the Inspector General's (OIG) Draft Evaluation Report and the OIG's recognition of the Department's continued progress in addressing weaknesses and enhancing its unclassified cybersecurity program. The information in this report will enable the OCIO and program offices to take appropriate follow-up action on specific findings, as well as to continue to work in the most effective way to improve the Department's cybersecurity posture.

With respect to the specific recommendations in this draft report:

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

Concur. The issues in this report have been identified in current and prior years' program and site evaluations. Plans of Action and Milestones (POA&Ms) have been developed; corrective actions cited in response to each of the OIG's previously issued evaluations and reports are in progress. In some cases, corrective actions have already been completed since the preparation of your draft report. With respect to the cybersecurity weaknesses that were not reported in POA&Ms, please provide detailed documentation to the programs and OCIO so that appropriate actions can be taken.

Recommendation 2. *Ensure that procedures and processes are developed, as needed, and implemented in accordance with Federal and Department requirements to adequately secure systems and applications.*

Concur. DOE Order 205.1B, Department of Energy Cyber Security Program requires Senior DOE Management (SDM) Organizations to develop and implement procedures and processes for securing information, information systems and applications. DOE O



Printed with soy ink on recycled paper

205.1B was signed by the Deputy Secretary on May 16, 2011. The revised Order promulgates the governance structure established by the Deputy Secretary in December 2009, codifies DOE's approach for risk management and incorporates requirements of existing cybersecurity Manuals and aligns requirements with National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) standards. Efforts continue in FY 2012 with ongoing reviews of other existing cybersecurity program directives such as the Incident Management Order and the Telecommunications Security Program Order.

Recommendation 3. Ensure that effective performance monitoring practices are implemented to assess overall performance for protecting information technology resources.

Concur. DOE Order 205.1B, Department of Energy Cyber Security Program requires Senior DOE Management (SDM) Organizations to develop and implement performance monitoring practices for assessing overall performance of protecting information, information systems and applications. The Department Cybersecurity Program is founded on the DOE Risk Management Approach (RMA), which has been codified in DOE O 205.1B, dated: May 16, 2011. The implementation of 205.1B is handled by the Senior DOE Management Organizations, which flow down the requirements and responsibilities to all subordinate organizational levels through implementation plans (RMA Implementation Plans / Program Cyber Security Plans (PCSP)). These RMA plans include the implementation of contractor assurance systems, which demonstrate risk is being identified and mitigated to an acceptable level in accordance with mission.

Cybersecurity oversight is accomplished at the SDM-level.

Recommendation 4. Ensure that POA&Ms are developed and used to prioritize and track remediation of all cyber security weaknesses requiring corrective actions.

Concur. The OCIO coordinates with the Department's Program/Staff Offices, which provide quarterly POA&M updates. The updating, tracking and prioritizing of POA&MS still rely on sustained SDM-level attention to remediation of identified weaknesses. The OCIO tracks both program and system-level updates. The OCIO has selected an Enterprise tool that will provide a centralized repository for tracking Program/Staff Offices cybersecurity weaknesses and remediation activities. The tool will improve accuracy and ease reporting of POA&Ms. OCIO will work with Audit Organizations to confirm that all audit findings are recorded and tracked as POA&Ms.

If you have any questions or need additional information, please contact me or Mr. Gil Vega, Associate Chief Information Officer for Cybersecurity, at (202) 586-0166.




Department of Energy
National Nuclear Security Administration
Washington, DC 20585



October 14, 2011

MEMORANDUM FOR: RICKEY R. HASS
DEPUTY INSPECTOR GENERAL
FOR AUDIT AND INSPECTIONS
OFFICE OF INSPECTOR GENERAL

FROM: 
KENNETH W. POWERS
ASSOCIATE ADMINISTRATOR
FOR MANAGEMENT AND BUDGET

SUBJECT: Comments to the IG's Draft Report on FISMA – 2011;
Project No. A11TG029; IDRMS No. 2011-00287

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 – 2011*. I understand that this audit was performed to determine whether the Department's unclassified cyber security program adequately protected its information and systems.

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. At the same time, we disagree with the IG's characterization of the scope, severity, and cause of the issues presented in this report. Specifically:

- The information systems within the Nuclear Security Enterprise (NSE) are enormous in number and vary in scope. The sites the IG visited this year alone have a significantly large number of computing devices under their purview. The fractional percentages of misconfigured devices identified are isolated issues at the system-level and not across the NSE as could be concluded by the casual reader of the report. Also, the IG reviews performed under this report do not indicate if the misconfigured machines or policy deficiencies are within a site's acceptable risk envelope or the degree that compensating controls or mitigating elements protect systems from cyber attacks.
- Previous efforts to implement security controls consistently throughout the Federal Government applied federally mandated methods that focused security protections and resources on compliance with specific controls and technologies developed to address threats and risks identified years ago. The National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) just recently updated and issued harmonized policies, instructions, standards and guidelines supporting a unified risk-based information security framework for the federal government to be able to implement cost-effective security controls/investments that are based on the degree of



Printed with soy ink on recycled paper

protections consistent with Agency's respective missions, aligned with current threats, and agility in the face of changing threats. However, audits continue to be based upon system compliance checklists and not according to current cyber security methodologies that target the strength of layered defense strategies that will effectively mitigate some of the risks to an acceptable level and significantly reduce the cost and burden of implementation and maintenance of certain security controls at the system-level.

- All NNSA systems are protected by distinctive, layered, and defense in-depth approaches. The finding of a particular technical misconfiguration, alone, does not necessarily translate to substantive 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 implementation to include firewalls, intrusion detection, antivirus, network monitoring, and physical security that is operated 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 represent demonstrated risks as the reviews conducted targeted security controls only at the system-level with no further investigation into the layered defenses deployed at the site or enterprise level.
- NNSA's information systems are managed in large part by managing and operating (M&O) contractors with Federal oversight. NNSA sites recognize different levels of risk, implement strategies to mitigate those risks based upon sound risk management principles, and where appropriate, accept a certain level of risk depending on the unique circumstances of the sites and systems. Securing systems is complex and variable, and NNSA undertakes significant effort to prevent and respond to security findings/incidents/advanced threats. It is important that the complete health of the Department's cyber program is accurately reported according to the type and level of evaluation performed. As such, when describing a deficiency, the description must adequately characterize the impact of the potential exposure as it relates to that specific workstation, server, network and enterprise. While finding deficiencies is important, we should be careful not to overstate the impact of a few instances of misconfigured devices against the backdrop of wide ranging and complex infrastructure.

Therefore, while we support the IG's efforts in this area, we are concerned that the casual reader of this report may lack the context, technical cyber security knowledge, and risk management expertise required to draw accurate conclusions regarding NNSA's stewardship of unclassified information technology assets. We would therefore ask that the IG consider adjusting the report to provide a more balanced context for the findings and recommendations as noted above.

Below are the NNSA responses to the recommendations outlined in the draft report.

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

Concur. The findings identified under this report are system-level issues and will need to be corrected through implementation of appropriate controls by the applicable site M&O. This finding is inappropriately assigned to the Under Secretary for Nuclear

Security as stated. However, the NNSA's Chief Information Office (CIO), working in concert with the NNSA Site Offices, will further review cyber security activities maintained by M&Os and adequately rectify specific control weaknesses that are not within the acceptable risk envelope. Estimated completion of actions is December 31, 2012.

Recommendation 2: *Ensure that procedures and processes are developed, as needed, and implemented in accordance with Federal and Department requirements to adequately secure systems and applications.*

Concur. The NNSA CIO is currently developing policies and procedures to ensure deficiencies outlined in this report, which were identified at the system or operations level, will be corrected by the applicable site M&O, along with the implementation of their risk management framework. The NNSA CIO working in concert with the M&O CIOs will ensure that site cyber security policy and procedures to address the system and operational level deficiencies in accordance with Departmental requirements. Estimated completion of actions is December 31, 2012.

Recommendation 3: *Ensure that effective performance monitoring practices are implemented to assess overall performance for protecting information technology resources.*

Concur. The risk management approach and implementation of a contractor assurance model is intended to specifically address the elements of this recommendation. Actions in this area will be consistent with the direction set by the Administrator and Deputy Administrator for transforming oversight activities within NNSA. 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. Estimated completion of actions is December 31, 2012.

Recommendation 4: *Ensure that POA&Ms are developed and used to prioritize and track remediation of all cyber security weaknesses requiring corrective actions.*

Concur. The NNSA CIO will evaluate changes which need to be made in the organization's POA&M program to better align contractor assurance systems and federal corporate performance systems with the concepts of POA&M and Risk Management reflected in Federal Guidance and CyberScope requirements. Estimated completion of actions is December 31, 2012.

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

cc: Robert Osborn, Chief Information Officer
Wayne Jones, Deputy Chief Information Officer

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://energy.gov/ig>

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