



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

# Evaluation Report

---

## The Department of Energy's Unclassified Cyber Security Program – 2013

DOE/IG-0897

October 2013



**Department of Energy**  
Washington, DC 20585

October 29, 2013

MEMORANDUM FOR THE SECRETARY

FROM:   
Gregory H. Friedman  
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department of Energy's  
Unclassified Cyber Security Program – 2013"

BACKGROUND

Cyber security threats are a major concern for all Federal entities, including the Department of Energy. Several recent cyber attacks against the Department's networks and systems have underscored the importance and urgency of a strong cyber security program. For instance, a recent attacker exploited a known vulnerability resulting in the compromise of personally identifiable information for over 100,000 current and former employees, employee dependents and contractors.

The *Federal Information Security Management Act of 2002* (FISMA) established the requirement for Federal agencies to develop, implement and manage agency-wide information security programs, and provide acceptable levels of security for the information and systems that support the operations and assets of the agency. Systems that support Federal missions and are funded by the Department but managed or operated by contractors also fall under the purview of FISMA. As part of our responsibilities under FISMA, the Office of Inspector General conducts an annual independent evaluation to determine whether the Department's unclassified cyber security program adequately protected its unclassified data and information systems. This report documents the results of our evaluation for Fiscal Year (FY) 2013.

RESULTS OF EVALUATION

The Department had taken a number of positive steps over the past year to correct cyber security weaknesses related to its unclassified information systems. This included corrective actions to resolve 28 of the 38 conditions we identified during our FY 2012 evaluation. In addition, the Department established a senior leadership council to increase high-level visibility of cyber-related issues.

In spite of these efforts, we found that significant weaknesses and associated vulnerabilities continued to expose the Department's unclassified information systems to a higher than necessary risk of compromise. While weaknesses identified as a result of Office of Inspector General vulnerability scanning decreased somewhat during our FY 2013 evaluation, those related to general information technology controls increased. Our testing revealed various weaknesses related to security reporting, access controls, patch management, system integrity,

configuration management, segregation of duties and security management. In total, we discovered 29 new weaknesses and confirmed that 10 weaknesses from the prior year's review had not been resolved. These problems were spread across 11 of the 26 Department locations where we performed testing. Specifically:

- We discovered 11 access control deficiencies at 8 facilities related to inadequate management of user access privileges, inappropriate granting of physical access to sensitive facilities, failure to implement multi-factor authentication for remote access and use of default or easily guessed login credentials on servers or network services.
- At five locations, we determined that weaknesses existed related to vulnerability management of desktop computers and network systems. These findings were primarily focused on vulnerable operating systems and applications that were missing security updates and/or patches. Weaknesses of this sort directly contributed to the recent compromise and exfiltration of personally identifiable information on over 100,000 individuals from one of the Department's systems.
- Weaknesses related to system integrity of web applications, including improper validation of input data and unsecured user authentication information that support financial management and general support functions, were identified at six locations.
- We identified five weaknesses related to configuration management at three locations. The weaknesses included failure to develop or document an organizational configuration management policy, inconsistent implementation of configuration change control procedures and inadequate management of application change control processes.
- At one site, we found weaknesses related to segregation of duties. Specifically, established procedures governing the roles and responsibilities assigned to system users were not always followed.
- Finally, we identified several security management program weaknesses at three sites associated with ensuring that all employees had taken security training, cyber security incidents were reported, a system inventory was maintained, and audit logs were reviewed.

Notably, despite requirements established in FISMA implementing guidance promulgated by the Office of Management and Budget, the Department had not included contractor-owned/operated systems when reporting performance metrics related to the health of its cyber security program to the Department of Homeland Security. Specifically, the Department did not report detailed security information for more than 450 systems operated by its contractors. Given the fact that the majority of the vulnerabilities we discovered during this review and in past years involved contractor-operated systems, such disclosures are both relevant and necessary.

The weaknesses we identified occurred, in part, because Department elements had not ensured that policies and procedures were fully developed and implemented to meet all necessary cyber security requirements. In addition, the Department continued to operate a less than fully effective performance monitoring and risk management program. For example, locations

reviewed had not always followed program or site-level patch management policies and procedures to ensure security updates were applied in a timely manner. Programs and sites also had not consistently followed existing policies related to terminating or disabling user access when no longer needed. Furthermore, we found that 24 of the 38 (63 percent) weaknesses identified in our prior year review were not tracked in the Department's Plan of Actions and Milestones. Absent improvements to its unclassified cyber security program, the Department's information and systems will continue to be at a higher than necessary risk of compromise. As such, we made several recommendations that, if fully implemented, should help the Department strengthen its cyber security program.

Due to the sensitive nature of the vulnerabilities identified during our evaluation, specific information and site locations have been omitted from this report. Site and program officials have been provided with detailed information regarding the vulnerabilities that were identified at their sites and, in many cases, initiated corrective actions to correct the identified deficiencies.

We are conducting a criminal investigation and a separate special inquiry into the July 2013 intrusion and theft of personally identifiable information from the Department. The results of our inquiry will be reported separately.

#### MANAGEMENT REACTION

Management concurred with the report's findings and recommendations and had taken and/or initiated corrective actions. Management's comments and our response are summarized and more fully discussed in the body of the report. Management's formal comments are included in Appendix 3.

Attachment

cc: Deputy Secretary  
Acting Under Secretary for Nuclear Security  
Acting Under Secretary for Science and Energy  
Acting Under Secretary for Management and Performance  
Chief Information Officer  
Acting Chief Financial Officer  
Director, Office of Management

**EVALUATION REPORT ON THE DEPARTMENT OF ENERGY'S  
UNCLASSIFIED CYBER SECURITY PROGRAM – 2013**

---

**TABLE OF  
CONTENTS**

**Security Controls and Risk Management**

Details of Finding ..... 1

Recommendations ..... 8

Management Response and Auditor Comments ..... 9

**Appendices**

1. Objective, Scope and Methodology ..... 10

2. Related Reports ..... 12

3. Management Comments ..... 15

# THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBER SECURITY PROGRAM – 2013

---

## Program Improvements

The Department of Energy (Department), including the National Nuclear Security Administration (NNSA), had taken a number of steps over the past year to address previously identified cyber security weaknesses and enhance its unclassified cyber security program. In particular:

- The Department had taken corrective action to resolve or mitigate a number of previously identified vulnerabilities at 11 locations. Actions taken addressed weaknesses related to access controls, configuration and vulnerability management, system integrity, incident reporting and contingency planning. In fact, the number of weaknesses identified during our current review that were attributable to technical system vulnerabilities such as patch management had decreased by about one-third when compared to last year's review.
- The Department established an executive-level Cyber Council as the principal forum for coordination of its cyber-related activities across the enterprise and for consideration of issues requiring a decision by the Secretary of Energy. Such activities addressed protecting the enterprise, including the Department's management and operating contractors, from a range of cyber threats, bolstering the Government's capabilities to address such threats, and improving cyber security in the electric power, oil and natural gas subsectors. Membership in the Council consisted of executive-level leadership from the Department's program and staff offices.
- The Department's programmatic elements and field sites had made improvements in the implementation of Homeland Security Presidential Directive-12 and the development of a risk management approach for cyber security programs. For example, Department Order 206.2, *Identity, Credential, and Access Management*, was issued in February 2013, in response to our report on *The Department of Energy's Implementation of Homeland Security Presidential Directive 12* (DOE/IG-0860, February 2012). This directive promulgated policy related to the issuance of credentials for uncleared contractors; an issue identified in our February 2012 report. In addition, programs and sites continue to work towards effective implementation of a risk management approach.

Although the actions taken by the Department over the last year should help improve its cyber security position, our current evaluation found that programs and sites must continue to remain cognizant of constantly changing and emerging threats and the potential impact these issues pose to unclassified information systems and data.

## Security Controls and Risk Management

The current evaluation identified an area of concern regarding the completeness of the Department's performance metrics reporting to the Department of Homeland Security related to the health of its cyber security program. Although the Department had made progress correcting

---

deficiencies we identified in our Fiscal Year (FY) 2012 evaluation, additional effort is needed to enhance its unclassified cyber security program and further mitigate the risks to its information and systems. Specifically, while the number of findings issued as a result of our vulnerability scanning decreased from our FY 2012 review, we identified an increased number of weaknesses related to general information technology controls than in past years.

Our review of Under Secretary of Nuclear Security, Under Secretary for Science and Energy and Under Secretary for Management and Performance organizations identified various weaknesses related to security reporting, access controls, patch management, system integrity of web applications, configuration management, segregation of duties and security management. Based on the results of our FY 2013 evaluation, 29 new weaknesses and 10 unresolved weaknesses from the prior year's review were identified at 11 of 26 locations included in our current year evaluation.

### Security Reporting

The Department's cyber security performance metric reporting, which is provided to the Department of Homeland Security under the requirements of the *Federal Information Security Management Act of 2002*, did not include information related to Department funded, contractor managed/operated information systems. The Department reported in FY 2012 that 469 of its 649 (72 percent) information systems belong to or are managed by contractors. However, the information provided to the Department of Homeland Security in response to the FY 2012 performance metrics stated that it was based only on Federal systems. Thus, the Department underreported the results of its cyber security program in seven critical areas, including asset management, configuration and vulnerability management, identity and access management and data and boundary protection. This resulted in reduced visibility of the level of security over the vast majority of the Department's information systems, limiting the ability to implement an effective complex-wide risk management process. While a Department official told us that security information for contractor systems would be reported beginning in FY 2013, we were unable to confirm whether this had occurred at the time of our review.

### Access Controls

Although the Department had taken action to correct a number of prior year access control weaknesses, we continued to identify issues related to logical and physical access controls at numerous locations. Access controls consist of both physical and logical measures designed to protect information resources from unauthorized modification, loss or disclosure. Controls must be strong and functional to ensure that only authorized individuals can gain access to networks and systems or the facilities in which they are located. During our FY 2013 review, we identified 12 access control deficiencies at 8 locations. In particular:

- Eight account management weaknesses were identified at six locations, including inadequately managed user access privileges and failure to perform periodic management reviews of user accounts. For instance, access privileges at six locations were not appropriately established, modified, reviewed, disabled and/or removed. All six locations failed to remove terminated or inactive user accounts in a timely manner. One site had

---

not disabled all inactive users who had not logged into the system within the past 60 days despite the requirement to do so. At another site, user accounts with elevated privileges remained active even though users had not logged in for more than 3 years.

- One site had inappropriately granted physical access to a data center where information systems were maintained. Specifically, an individual was granted access to the data center when such access was not required to perform job duties. The individual had not accessed the data center, and management took corrective action to remove this access when we brought this matter to its attention.
- Although one site had implemented tools necessary to ensure that remote access to its network and information systems was secure or properly protected, several remote access weaknesses were identified at the site. We found that multi-factor authentication for privileged users had not been implemented, and full disk encryption security measures had not been activated on mobile computers, including some that could potentially contain sensitive data such as personally identifiable information. Furthermore, five remote access accounts belonging to terminated users had not been properly disabled in a timely manner.
- One site had 11 network server systems and devices that were configured with default or easily guessed login credentials or that required no authentication for access. These configuration vulnerabilities could have allowed an attacker to obtain unauthorized access to the affected devices and the data stored on them. Furthermore, some of the vulnerabilities could have allowed malicious programs to attack other systems on the internal network. Although the site had updated policies and procedures designed to address the identified weakness, we noted that implementation of the policies and procedures was not effective.
- One site maintained seven servers/systems running network services that were configured with open access settings that could have allowed remote systems to obtain access to data on the system without the use of login credentials. Sensitive financial data and personnel payroll information was accessible through one of those servers. Once the site became aware of the issue, management took corrective action to restrict access and remove sensitive data from servers that had open access settings.

### Patch Management

The Department had made improvements in its patch management program since our prior year review. However, we continued to identify issues related to patch management of desktop computers and network systems at six locations. The weaknesses consisted of varying degrees of vulnerable applications and operating systems missing security updates and/or patches, including 3 critical and more than 200 high-risk vulnerabilities. Site and management officials told us that they had accepted the risks associated with many of the vulnerabilities; however, they could not always provide documentation to support a risk acceptance decision. We also noted that in a number of cases, compensating controls were insufficient to address the observed vulnerabilities. In particular:

- 
- Scans of desktop systems at 17 locations revealed that 965 of 2,357 (41 percent) systems were running operating systems and/or client applications without current security patches for known vulnerabilities. The vulnerable client applications included media players and productivity and remote access software and were missing security patches for known vulnerabilities that had been released more than 30 days prior to our testing. At one site, nearly every desktop system scanned contained outdated applications. Our testing of workstations targeted users with elevated privileges and was a small subset of all workstations at the sites reviewed. Therefore, we consider the results of our testing to be very conservative.
  - More than 100 network systems tested were running operating systems and application support platforms without current security patches or security configurations for known vulnerabilities that were released more than 30 days prior to testing. We also identified 23 network server systems running operating system versions that were no longer supported by the vendor.

The danger of unpatched systems was demonstrated in July 2013, when an unpatched application provided the vector for attackers to breach a system at Headquarters containing significant amounts of sensitive information. As a result, personally identifiable information for more than 100,000 current and former employees, employee dependents and contractors was exfiltrated. We are conducting a criminal investigation into this matter and are in the process of performing a special inquiry into the circumstances that contributed to the event. We will issue a separate report detailing the results of our special inquiry.

#### System Integrity of Web Applications

We identified eight weaknesses related to system integrity of web applications at six locations. Our performance testing found web applications – including financial, human resources and general support applications – that did not perform validation procedures to determine whether the form and content of input data was validated against an application's database. Effective validation procedures can 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 software flaws and malicious code. We found:

- At six locations, applications that accepted malicious input data could be used to launch attacks against legitimate users, resulting in unauthorized access. Such attacks, referred to as cross-site scripting, could result in a compromise of legitimate users' workstations and application login credentials. Notably, weaknesses at three of the six locations were initially identified during prior year reviews, but had not been fully remediated and were still considered vulnerable to the aforementioned attacks. Upon notification of our findings, some sites had initiated and/or completed corrective actions.

Two locations stored unsecured user authentication information on the network. These identifiers were accessible to any web server within the same network. Thus, unsecured user authentication information stored in a user's web browser could be exposed to

---

attackers or unauthorized users through attacks executed against any web server within the network. These weaknesses could also allow an attacker to compromise legitimate users' workstations and application login credentials.

Unsecured web applications, such as those identified during our testing, increase the risk of malicious attacks that could result in unauthorized access to application functionality and sensitive data stored in the application.

### Configuration Management

We identified five weaknesses related to configuration management of information systems at three locations. The weaknesses involved inadequate implementation of configuration change control procedures, failure to develop standard baseline configurations for all systems and insufficient documentation of application change controls. Specifically:

- At two sites, we found that configuration change control procedures had not been implemented consistently even though procedures had been documented. For example, we identified 15 changes to a firewall configuration at one site that were not in accordance with configuration management plan procedures. In addition, officials at another site had not documented, retained or reviewed information system changes. At that site, we were unable to obtain or review changes implemented in FY 2013. As such, we could not determine whether changes were adequately documented, tested and approved prior to implementation.
- One site had not developed or documented an organizational configuration management policy and related procedures for managing hardware and software. Even though the site maintained standard baseline configurations for centrally managed operating systems and applications, we found that a minimum security configuration policy and requirements for non-centrally managed systems had not been established or documented.
- One site had weaknesses related to managing its application change control process. Although the site used an application to track and monitor configuration changes, we found that change requests for the application had not been documented and maintained. Rather, all change requests had been made verbally to the developer, and no change control forms had been completed. When informed of our findings, management took corrective actions to update plans and procedures.

### Segregation of Duties

We identified a weakness related to segregation of duties at one location. Specifically, several individuals were assigned responsibilities that conflicted with the organization's documented separation of duties rules. As an example, one individual was able to enter purchase order information and had accounts payable invoicing rights. In total, 12 individuals had been assigned roles that could have allowed an increased risk of unauthorized activities without collusion when processing transactions. When informed of our findings, management took corrective action to address the users' conflicting roles.

---

## Security Management

We identified several security management weaknesses at three locations related to ensuring all employees had taken security training, all cyber security incidents were reported, system inventories were maintained and audit logs were reviewed. In particular:

- Two locations had not provided adequate security training to all employees. For example, at one site, approximately 500 users had not taken a security training course even though it was required by site-level policy. At another site, officials had not identified individuals required to take specialized security training and ensured that such training had occurred.
- Two sites had weaknesses related to incident response, asset management and audit logging and monitoring. Specifically, we found that lost or potentially stolen information technology equipment at one site had not been properly reported by the site to the Department's Joint Cyber Security Coordination Center. Another location had not maintained a complete inventory of all information systems and had not reviewed system logs to identify anomalies in access or activity.

## **Policies and Procedures, Performance Monitoring and Risk Management**

The weaknesses identified occurred because Department elements had not ensured that policies and procedures were fully developed and implemented to meet all necessary cyber security requirements. In addition, the Department continued to operate a less than fully effective performance monitoring and risk management program.

### Policies and Procedures

Consistent with our prior year reviews, sites developed cyber security policies and procedures that were inadequate or did not always satisfy Federal or Department security requirements. For instance, we noted that policies and procedures at certain locations did not clearly designate the responsible parties for reporting lost or stolen laptops, resulting in security incidents not being reported in a timely manner. Similar issues were identified in our *Follow-up Audit of the Department's Cyber Security Incident Response Program* (DOE/IG-0878, December 2012).

Even when in place, policies and procedures were not always fully implemented. For instance, locations reviewed had not always followed program or site-level patch management policies and procedures to ensure security updates were applied in a timely manner. Furthermore, programs and sites had not consistently followed existing policies related to terminating or disabling user access when no longer needed. In one instance, although the site's policies required deletion or deactivation of user accounts that had been inactive for 180 days, we found that more than 100 accounts were active for more than 6 months even though they were unused. In addition, we found that some sites had updated policies and procedures related to security training, but these changes had not always been fully implemented to ensure all users were trained.

---

## Performance Monitoring and Risk Management

The Department continued to operate a less than fully effective performance monitoring and risk management program. In particular, many of the programs and sites reviewed had not fully implemented an effective process to ensure security patch management processes for desktop computers, network devices and applications were working as designed. For instance, we found that vulnerability management programs at numerous locations were not always effective in remediating missing security updates for critical vulnerabilities in operating systems and applications installed on network systems and/or workstations. In addition, many of the web application vulnerabilities we identified occurred because programs and sites had not implemented effective processes to ensure that controls were in place to identify and prevent application integrity issues. At two sites where prior year weaknesses remained, input data validation safeguards had not been effectively developed and implemented as part of application functionality. As the Department continues its efforts to implement a cyber security continuous monitoring program, it is essential that adequate performance monitoring mechanisms are in place.

Contrary to Federal requirements, we also found that plans of action and milestones were not always effectively used as a monitoring tool to report, prioritize and track cyber security weaknesses. The use of plans of action and milestones is an important mechanism to identify and manage progress towards eliminating gaps between required security controls and those that are actually in place. However, we found:

- Although many of the sites reviewed tracked weaknesses at a local level, cyber security deficiencies identified during our FY 2012 review were not always included. In particular, 22 of 38 (58 percent) weaknesses identified last year were not tracked in the plans of action and milestones submitted to the Office of the Chief Information Officer. As a result, these issues were not reported to the Office of Management and Budget, as required. Perhaps more importantly, the Department's Chief Information Officer did not have visibility over the critical weaknesses in the Department's cyber security program. We also noted that plans of action and milestones did not contain all cyber security weaknesses identified in numerous security related Office of Inspector General reports.
- As compared to our FY 2012 evaluation, we noted an increase in the number of open milestones in the plans of actions and milestones that were beyond the projected remediation date. Specifically, we determined that 467 of 921 (51 percent) open milestones were beyond the projected remediation date, including 133 open milestones that were at least 1 year beyond the estimated remediation date.

We also identified several concerns related to the ability to implement risk management practices. For example, one site had not completed documentation supporting its risk management process and acceptance of risk associated with web application vulnerabilities. The site also had not documented residual risk, business justifications and mitigations for vulnerabilities that were identified by system scanning tools. In addition, we found that Department officials misunderstood a Department of Homeland Security memorandum that led

---

them to report only limited information on contractor systems, resulting in reduced visibility of security over the vast majority of the Department's information systems and limiting the ability to implement an effective complex-wide risk management process. According to a Department official, security information for contractor systems will be reported beginning in FY 2013; however, at the time of our review, we were unable to confirm whether this had occurred. As the Department continues its efforts to rely on contractor assurance processes for monitoring the effectiveness of programs, it is essential that adequate performance monitoring mechanisms are in place.

## **Risk to Information and Systems**

As in years past, we note that without changes to improve the operation of its cyber security program, including implementing effective policies and procedures and enhancing performance monitoring, the Department's information systems and data will continue to be at risk. Recently, this point was made clear when an unpatched Department application was exploited, allowing attackers to breach a Headquarters' system and exfiltrate personally identifiable information for more than 100,000 current and former Department employees, employee dependents and contractors.

In addition, without knowledge of security over contractor operated systems, the Department's information and systems will continue to be at risk as threats constantly change. Although programs and sites had implemented mitigating controls in certain instances, we found that the weaknesses identified during our review could potentially be exploited by attackers. As such, effective remediation of the weaknesses identified during our review should help the Department strengthen its cyber security program. The remediation process could be further improved through effective implementation of the plan of actions and milestones process. Comprehensive plan of actions and milestones would allow officials to identify security risks and determine what type of action should be taken to address them in an efficient and prioritized manner.

## **RECOMMENDATIONS**

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

1. Correct, through the implementation of appropriate controls, the weaknesses identified within this report;
2. Ensure that policies and procedures are developed, as needed, and are 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;

- 
4. Fully develop and use plans of actions and milestones to prioritize and track remediation of all cyber security weaknesses requiring corrective actions; and
  5. Ensure that the Department includes information for both Federal and contractor systems when reporting the status of performance metrics annually to the Department of Homeland Security.

## **MANAGEMENT RESPONSE**

Department management concurred with each of the report's recommendations and indicated that corrective actions would be identified and tracked in the appropriate plans of action and milestones. For instance, the Office of the Chief Information Officer indicated that it is piloting an automated tool to provide a centralized repository for tracking program and system-level cyber security weaknesses and remediation activities. In addition, management commented that it enhanced performance monitoring activities and will include both Federal and contractor compliance information as part of the FY 2013 reporting to the Office of Management and Budget. In separate comments, NNSA management concurred with the recommendations and planned to take corrective actions to resolve the weaknesses identified in our report.

## **AUDITOR COMMENTS**

Management's comments were responsive to our recommendations. Management's comments are included in Appendix 3.

### OBJECTIVE, SCOPE AND METHODOLOGY

#### OBJECTIVE

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

#### SCOPE

We conducted the evaluation from February 2013 to October 2013 at 26 Department locations under the responsibility of the Under Secretary of Nuclear Security, Under Secretary for Science and Energy and the Under Secretary for Management and Performance. The focus of our evaluation was the Department's unclassified cyber security program. This work involved a limited review of general and application controls in areas such as security management, access controls, configuration management, segregation of duties and contingency planning. Where vulnerabilities were identified, the evaluation did not include a determination of whether the vulnerabilities were actually exploited.

#### METHODOLOGY

To accomplish the audit objective, we:

- Reviewed Federal regulations and Department directives pertaining to information and cyber security.
- Reviewed applicable standards and guidance issued by the National Institute of Standards and Technology for the planning and management of system and information security.
- Obtained and analyzed documentation from Department programs and selected sites pertaining to the planning, development and management of cyber security related functions such as cyber security plans, plans of action and milestones and budget information.
- Held discussions with officials from the Department and the National Nuclear Security Administration.
- Assessed controls over network operations and systems to determine the effectiveness related to safeguarding information resources from unauthorized internal and external sources.
- Evaluated selected Headquarters' offices and field sites in conjunction with the annual audit of the Department's Consolidated Financial Statements, utilizing work performed by KPMG, LLP (KPMG), the Office of Inspector General's contract auditor. Office of Inspector General and KPMG work included analysis and testing of general and application controls for systems, as well as vulnerability and penetration testing of networks.

## Appendix 1 (continued)

---

- Evaluated and incorporated the results of other cyber security review work performed by the Office of Inspector General, KPMG, the U.S. Government Accountability Office and the Office of Health, Safety and Security's Office of Enforcement and Oversight.

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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. In particular, we assessed the Department's implementation of the *GPR Modernization Act of 2010* and determined that it had established performance measures for its information and cyber security program. Because our evaluation was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did not solely rely on computer-processed data to satisfy our objective. However, computer assisted audit tools were used to perform scans 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 Office of the Chief Information Officer and the National Nuclear Security Administration both waived an exit conference.

### RELATED REPORTS

#### Office of Inspector General Reports

- Audit Report on [\*Management of the Naval Reactors' Cyber Security Program\*](#) (DOE/IG-0884, April 2013). The Office of Inspector General (OIG) found that, although the Naval Reactors Program (Naval Reactors) had made a number of enhancements to its cyber security program over the past year, we identified weaknesses related to vulnerability management, access controls, incident response and security awareness training that could negatively affect its security posture. The weakness identified occurred, in part, because Naval Reactors had not ensured that necessary cyber security controls were fully implemented. Specifically, officials had not fully developed and/or implemented policies and procedures related to vulnerability management, access controls, incident response and cyber security training. In addition, Naval Reactors had not always effectively utilized plans of action and milestones to track, prioritize and remediate cyber security weaknesses.
- Audit Report on [\*Management of Los Alamos National Laboratory's Cyber Security Program\*](#) (DOE/IG-0880, February 2013). The OIG found that Los Alamos National Laboratory (Los Alamos) had taken steps to address concerns regarding its cyber security program raised in prior evaluations. However, we identified continuing concerns related to Los Alamos' implementation of risk management, system security testing and vulnerability management practices. The issues identified occurred, in part, because of a lack of effective monitoring and oversight of Los Alamos' cyber security program by the Los Alamos Site Office, including approval of practices that were less rigorous than those required by Federal directives. In addition, we found that Los Alamos' Information Technology Directorate had not followed National Nuclear Security Administration policies and guidance for assessing system risk and had not fully implemented the Laboratory's own policy related to ensuring that scanning was conducted to identify and mitigate security vulnerabilities in a timely manner.
- Report on [\*Management Letter on the Audit of the Department of Energy's Consolidated Financial Statements for Fiscal Year 2012\*](#) (DOE/OAS-FS-13-08, January 2013). Based on the audit of the consolidated financial statements of the Department of Energy (Department) for the year ended September 30, 2012, we found unclassified network and information system security to be an area where there were significant deficiencies in internal controls. We noted network vulnerabilities and weaknesses in access and other security controls in the Department's unclassified computer information systems. The identified weaknesses and vulnerabilities increased the risk that malicious destruction or alteration of data or unauthorized processing could occur. The Department should fully implement policies and procedures to improve its network and information systems security.

## Appendix 2 (continued)

---

- Audit Report on [\*Follow-up Audit of the Department's Cyber Security Incident Management Program\*](#) (DOE/IG-0878, December 2012). The OIG found that although certain actions had been taken in response to our prior audit report, we identified several issues that limited the efficiency and effectiveness of the Department's cyber security incident management program and adversely impacted the ability of law enforcement to investigate incidents. The issues identified were due, in part, to the lack of a unified, Department-wide cyber security incident management strategy. In addition, changes to the Department's Incident Management policy and guidance may have adversely impacted overall incident management and response by law enforcement and counterintelligence officials. Also, we found that incident reporting to law enforcement was not always timely or complete, which hindered investigations into events. In the absence of an effective enterprise-wide cyber security incident management program, a decentralized and fragmented approach has evolved that places the Department's information systems and networks at increased risk.
- Evaluation Report on [\*The Department's Unclassified Cyber Security Program – 2012\*](#) (DOE/IG-0877, November 2012). The OIG found that the Department had taken steps over the past year to address previously identified cyber security weaknesses and enhance its unclassified cyber security programs. The overall number of identified vulnerabilities decreased from 56 weaknesses in the prior year's evaluation to 38 in 2012. Although the number of vulnerabilities identified was reduced, the types and severity of weaknesses continued to persist and remained consistent with prior years. The weaknesses involved problems with access controls, vulnerability management, integrity of web applications, planning for continuity of operations and change control management. The weaknesses identified occurred, in part, because Department elements had not ensured that cyber security requirements were fully developed and implemented. In addition, programs and sites had not always effectively monitored performance to ensure that appropriate controls were in place.
- Audit Report on [\*Management of Western Area Power Administration's Cyber Security Program\*](#) (DOE/IG-0873, October 2012). The OIG found the Western Area Power Administration had made a number of enhancements to its cyber security program since OIG's prior review. However, several weaknesses related to vulnerability management and security controls existed that could negatively impact its cyber security posture. Specifically, Western Area Power Administration had not always implemented cyber security controls designed to address known system vulnerabilities and ensured that access controls designed to protect its information systems and data were in place. The weaknesses identified occurred, in part, because Western Area Power Administration had not always implemented policies and procedures related to vulnerability and patch management. Specifically, while cyber security officials conducted regular scans on two of the systems reviewed, they did not always identify and correct known vulnerabilities. In addition, officials had not fully implemented policies and procedures related to managing access to systems and information, including deactivating and/or disabling unneeded user accounts in a timely manner.

## Appendix 2 (continued)

---

- Special Report on [\*Management Challenges at the Department of Energy –Fiscal Year 2013\*](#) (DOE/IG-0874, October 2012). Based on the work performed during Fiscal Year (FY) 2012, the OIG identified nine areas, including cyber security, which remained a management challenge for FY 2013.
- Audit Report on [\*The Department of Energy's Implementation of Homeland Security Presidential Directive 12\*](#) (DOE/IG-0860, February 2012). The OIG found that, despite 7 years of effort and expenditures of more than \$15 million, the Department had yet to meet all Homeland Security Presidential Directive 12 (HSPD-12) requirements. In particular, the Department had not fully implemented physical and logical access controls in accordance with HSPD-12. Furthermore, the Department had not issued HSPD-12 credentials to many uncleared contractor personnel at its field sites. We noted what we considered to be a lack of a coordinated approach among programs and sites related to implementation of HSPD-12 requirements. In particular, we found that guidance provided by management was fragmented and often inadequate to meet the goals of the initiative. In addition, ongoing efforts suffered from lack of coordination among programs and sites to determine the cost, scope and schedule of work required to implement HSPD-12 requirements. Several programs and sites visited also had not established budgets in an attempt to obtain funding to support HSPD-12 activities.
- Audit Report on [\*The Department's Configuration Management of Non-Financial Systems\*](#) (DOE/OAS-M-12-02, February 2012). The OIG found the Department had not implemented sufficient controls over its configuration management processes for non-financial systems. Specifically, security patches designed to mitigate system vulnerabilities had not been applied in a timely manner for desktops, applications and servers. In addition, organizations and sites reviewed had not always followed effective procedures to ensure that changes to systems and applications were properly tested and approved prior to implementation.

### Government Accountability Office Reports

- [\*CYBERSECURITY: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges\*](#) (GAO-13-462T, March 2013)
- [\*HIGH-RISK SERIES: An Update\*](#) (GAO-13-283 and GAO-13-359T, February 2013)
- [\*CYBERSECURITY: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented\*](#) (GAO-13-187, February 2013)
- [\*IT SUPPLY CHAIN: National Security-Related Agencies Need to Better Address Risks\*](#) (GAO-12-361, March 2012)
- [\*SOCIAL MEDIA: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate\*](#) (GAO-11-605, June 2011)

**MANAGEMENT COMMENTS**



**Department of Energy**  
Washington, DC 20585

October 17, 2013

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

FROM: ROBERT F. BRESE   
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General's Draft Evaluation Report on "The Department's Unclassified Cyber Security Program – 2013"

Thank you for the opportunity to comment on the Draft Evaluation Report, "The Department's Unclassified Cyber Security Program - 2013." The information in this report will enable the Department Chief Information Officer (CIO) 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 the Department responds:

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

**Response:** Concur.

The weaknesses noted in this report have been reviewed and corrective actions will be identified by the appropriate DOE Programs in Plan of Action and Milestones (POA&Ms) reports. Each DOE program will provide the estimated completion dates and corrective actions will be managed to completion by the Programs and updated through quarterly POA&M reporting to the DOE OCIO.

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

**Response:** Concur.

The Department of Energy (DOE) Order 205.1B, Chg 2, *Department of Energy Cyber Security Program*, requires Senior DOE Management (SDM) Organizations to flow down requirements and responsibilities to all subordinate organizational levels through Risk Management Approach (RMA) implementation plans. These RMA implementation



Printed with soy ink on recycled paper

plans include the development and implementation of procedures and processes to secure information, information systems and applications, and the development and implementation of performance measures to assess the effectiveness of the procedures and processes in accordance with the DOE RMA. Procedure and process weaknesses noted in this report have been reviewed by the SDM Organizations and corrective actions will be managed to completion by the Programs and updated through POA&M reporting to the DOE OCIO.

Currently, the DOE Order 205.1B is the only cybersecurity directive for the Department. Additional cybersecurity requirements, such as incident reporting, will be incorporated into future directives.

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

**Response:** Concur.

The SDM Organizations identify and implement the performance monitoring requirements and responsibilities for all subordinate organizational levels through RMA implementation plans. The RMA plans include the implementation of contractor assurance systems to demonstrate that risk is identified and mitigated to an acceptable level in accordance with the mission. The weaknesses in this report related to performance monitoring practices have been reviewed by the SDM Organizations and corrective actions will be identified in Program POA&Ms. The progress and completion of POA&Ms will be managed to conclusion by the Programs and updated through quarterly POA&M reporting to the DOE OCIO.

**Recommendation 4.** *Fully develop and use plans of actions and milestones to prioritize and track remediation of all cyber security weaknesses requiring corrective actions.*

**Response:** Concur.

The DOE OCIO coordinates program and system-level POA&M tracking and updates with the Department's Program/Staff Offices. The updating, monitoring, and prioritizing of POA&Ms relies on sustained SDM-level attention to ensure remediation of identified weaknesses. The progress and completion of POA&Ms from this and prior reports will be managed to conclusion by the Programs and updated through quarterly POA&M reporting to the DOE OCIO. The DOE OCIO will confirm that weaknesses noted in this report are recorded and tracked as POA&Ms.

Additionally, the DOE OCIO selected and is piloting an Enterprise tool to provide a centralized repository for tracking program and system-level cybersecurity weaknesses and remediation activities. The tool will improve accuracy and ease reporting of POA&Ms. Web-based training sessions are currently underway to support the Enterprise tool rollout.

**Recommendation 5.** *Ensure that the Department includes information for both Federal and contractor systems when reporting the status of performance metrics annually to the Department of Homeland Security.*

**Response:** Concur.

The FY13 annual FISMA report will include reporting on both Federal and contractor system compliance for many of the FISMA questions including all of the Cyber Cross Agency Priority (CAP) Goals. The FY13 annual FISMA report will be completed and submitted by the OMB required due date.

If you have any questions or need additional information, please contact Mr. Paul Cunningham, Deputy Associate Chief Information Officer for Cybersecurity at (202)-586-9805.



Department of Energy  
National Nuclear Security Administration  
Washington, DC 20585



October 4, 2013

MEMORANDUM FOR RICKEY R. HASS  
DEPUTY INSPECTOR GENERAL  
FOR AUDITS AND INSPECTIONS

FROM: CINDY LERSTEN  
ASSOCIATE ADMINISTRATOR  
FOR MANAGEMENT AND BUDGET

SUBJECT: Response to Draft Evaluation Report on "The Department's  
Unclassified Cyber Security Program – 2013"  
(Job Code A13TG019/IDRMS No. 2013-00228)

Thank you for the opportunity to review and comment on the subject draft report. The National Nuclear Security Administration (NNSA) appreciates the Office of Inspector General's (OIG) recognition of NNSA's efforts to address previously identified cyber security weaknesses and enhance its unclassified cyber security program. With that said, cyber security remains one of the most challenging management areas and NNSA will continue to drive improvement efforts based on effective risk management. I understand the OIG identified a total of 29 new issues and 10 issues which continued and/or reoccurred from prior years, with NNSA sites accounting for only eight of those 29 issues. Five corporate recommendations were identified for management action.

NNSA agrees with the recommendations provided by the OIG to further enhance NNSA's and the Department's cyber security practices. NNSA will take the noted actions to address recommendations one through four, and will close the recommendations concurrent with resolution and closure of the supporting site specific findings and action plans. The initial estimated completion date for these actions is March 31, 2014. In relation to recommendation five, NNSA does not disagree that information for both Federal and contractor systems should be included when reporting the status of performance metrics annually to the Department of Homeland Security. However, we would like to clarify that NNSA follows the Department of Energy (Department's) reporting requirements and will accommodate any changes to those requirements. As the corrective action is under the Department's purview, we consider this recommendation closed for tracking purposes.

As a general comment, we appreciate the challenges inherent in auditing this area and in presenting the findings in a clear manner which protects our cyber security interests. With that said, to improve the clarity of the information presented, we believe it would be helpful to provide a reconciliation table to capture the issues identified in the report aligned by issue



Printed with soy ink on recycled paper

## Appendix 3 (continued)

---

type/area, number of occurrences, number of sites impacted, etc. This would complement the narrative and support a clearer view of how the issues align across the Department.

Should you have any questions regarding this response, please contact Dean Childs, Director, Audit Coordination and Internal Affairs, at (301) 903-1341.

## 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 applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or 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 that 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 our office 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.