



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

EVALUATION REPORT

The Department of Energy's Unclassified
Cybersecurity Program – 2015

DOE-OIG-16-01

November 2015



Department of Energy
Washington, DC 20585

November 3, 2015

MEMORANDUM FOR THE SECRETARY

A handwritten signature in black ink, appearing to read "Rickey R. Hass".

FROM: Rickey R. Hass
Acting Inspector General

SUBJECT: INFORMATION: Evaluation Report: "The Department of Energy's
Unclassified Cybersecurity Program – 2015"

BACKGROUND

As evidenced by recent large-scale attacks on Federal information systems and data at various agencies, including the Office of Personnel Management and the Department of Energy (Department), cybersecurity threats continue to present significant challenges. The Office of Management and Budget also noted in its fiscal year (FY) 2014 report to Congress that the volume and sophistication of attacks against Federal systems continued to increase. In addition, the Department reported more than 720 incidents in FY 2015 related to security over its information systems. These incidents related to areas such as compromises of information systems, loss or theft of information technology equipment, and failure to adequately protect personally identifiable information.

The *Federal Information Security Management Act of 2002* established the requirement for Federal agencies to develop, implement, and manage agency-wide information security programs. Federal agencies are also required to provide acceptable levels of security for the information and systems that support their operations and assets. Recently, the *Federal Information Security Modernization Act of 2014*, signed into law on December 18, 2014, modified the scope of agency reporting requirements to include specific information about security threats, incident reporting, and cyber breach notifications. As mandated by each of these laws, the Office of Inspector General is responsible for conducting an annual independent evaluation to determine whether the Department's unclassified cybersecurity program adequately protected its data and information systems. This report documents the results of our evaluation for the Department for FY 2015.

RESULTS OF EVALUATION

The Department, including the National Nuclear Security Administration, had taken a number of positive steps over the past year to address previously identified cybersecurity weaknesses related to its unclassified cybersecurity program. Specifically, we noted that the Department made significant progress in remediating weaknesses identified in our FY 2014 evaluation,

which resulted in the closure of 22 of 26 reported deficiencies. While these actions were positive, our current evaluation found that the types of deficiencies identified in prior years, such as issues related to security reporting, vulnerability management, system integrity of Web applications, and account management continued to persist. We observed the following:

- Contrary to management's response to our prior year's evaluation, the Department did not report the status of its entire cybersecurity program to the Department of Homeland Security. Rather, officials excluded contractor systems in their reporting, which accounted for 430 of the Department's 588 systems (73 percent). Our evaluation identified that more than three-quarters of the performance metrics submitted had been completed for Federal systems only. Interestingly, while officials chose not to report on the status of cybersecurity over contractor systems, we found that 220 of 363 (60 percent) cybersecurity incidents encountered by the Department between March and August 2015 occurred at contractor-managed locations. Officials commented that prior Office of the Chief Information Officer leadership made the decision that contractor information would not be reported and noted that reporting the information would be reassessed in the future.
- Our current year's testwork determined that although a number of improvements had been made, weaknesses continued to exist related to vulnerability management. For instance, we found that more than 1,300 laptops, workstations, and servers at one location had not received antivirus updates in a timely manner.
- Weaknesses existed related to system integrity of Web applications, including human resources, financial, and business applications. We found that applications accepted malicious input data that could have been used to launch attacks against application users. In addition, applications at a number of locations stored user authentication information in an unsecure manner.
- Access control and segregation of duties weaknesses and opportunities for improvement were identified at five locations. For example, we determined that 18 individuals at 1 location were granted excessive privileges that were not necessary to perform assigned tasks. We also determined that opportunities for improvement existed at three sites related to management of user access privileges and ensuring performance of periodic reviews of user accounts.

The weaknesses identified occurred, in part, because the Department had not ensured that policies and procedures were fully developed and/or implemented to meet all necessary cybersecurity requirements. In addition, the Department had not always implemented an effective performance monitoring and risk management program. For instance, we continued to identify concerns with the Department's implementation of plans of action and milestones to track corrective actions for its vulnerability management programs. Furthermore, we noted that risk management processes at locations reviewed were not always effective to identify and remediate cybersecurity weaknesses.

Without improvements to its cybersecurity program, such as adherence to policies and processes to ensure security controls are fully implemented, the systems with vulnerabilities identified will continue to be at a higher-than-necessary risk of compromise, loss, and/or modification. Furthermore, absent an effective process for tracking and implementing corrective actions, the Department may not adequately address cybersecurity risks or prioritize investments to ensure protection of data and information systems. As such, we made several recommendations that, if fully implemented, should help strengthen the Department's cybersecurity 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 vulnerabilities that were identified at their locations, and in many cases, initiated corrective actions to address the identified deficiencies.

MANAGEMENT RESPONSE

Management concurred with the report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report. Management's comments and our responses are summarized in the body of the report. Management's formal comments are included in Appendix 3.

Attachments

cc: Deputy Secretary
Under Secretary for Science and Energy
Administrator, National Nuclear Security Administration
Deputy Under Secretary for Management and Performance
Chief of Staff
Chief Information Officer
Chief Financial Officer

EVALUATION REPORT: THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2015

TABLE OF CONTENTS

Evaluation Report

Details of Finding1

Recommendations.....8

Management Response and Auditor Comments.....9

Appendices

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

2. Related Reports12

3. Management Comments16

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2015

DETAILS OF FINDING

The *Federal Information Security Modernization Act of 2014* (FISMA) requires agency Offices of Inspector General (OIGs) to conduct independent evaluations of information security programs and practices to determine whether unclassified cybersecurity programs adequately protect information systems and data. In accordance with FISMA, we conducted extensive control testing and assessments of the unclassified cybersecurity programs at 22 Department of Energy (Department) locations under the purview of the Administrator, National Nuclear Security Administration, Under Secretary for Science and Energy, and Under Secretary for Management and Performance. In addition to conducting fieldwork activities that included testing of networks and applications, technical vulnerability scanning, and validating corrective actions to remediate prior year weaknesses, we relied on audit results from ongoing and prior OIG reports. We also considered the results of the Department's Office of Enterprise Assessments when reporting on the Department's cybersecurity program.

Our fiscal year (FY) 2015 evaluation identified that the Department had taken significant action to address a large number of the deficiencies noted during our prior year evaluation. For instance, several sites had taken corrective actions to remediate all prior year weaknesses at their locations. However, we determined that various weaknesses existed related to ensuring security over systems and information, including several deficiencies from our prior year evaluation that had not been corrected. Although the actions taken by the Department should help improve its cybersecurity posture, additional effort is needed to ensure that systems and information are adequately secured and the risks of operating systems are known.

Unclassified Cybersecurity Program

The current year evaluation continued to identify an area of concern related to the completeness of the Department's performance metrics reporting to the Department of Homeland Security and Office of Management and Budget regarding its cybersecurity posture. In addition, this year's evaluation identified weaknesses related to vulnerability management, system integrity of Web applications, and account management and segregation of duties. Based on the results of our FY 2015 testwork, we identified vulnerabilities at various locations reviewed, including a number of new weaknesses and several unresolved weaknesses from the prior year.

Security Reporting

Consistent with prior years, the Department did not report the results of its entire cybersecurity program, to include information related to contractor systems, within its FISMA performance metric submission to the Department of Homeland Security and Office of Management and Budget. This issue was first identified in our evaluation report on *The Department of Energy's Unclassified Cyber Security Program – 2013* (DOE/IG-0897, October 2013). Even though contractor-operated systems accounted for 430 of the Department's 588 systems (73 percent), our review of the Department's FY 2014 annual FISMA report identified that 61 of 78 metrics submitted had been completed for Federal systems only. Complete information in four critical areas related to identity and access management, data protection, boundary protection, and incident management was not submitted for contractor-managed and -operated systems. The

lack of information related to the Department's incident management activities, such as the percentage of events detected during penetration tests and the mean detection time of applicable events, could prevent the Department from making informed risk-based decisions about the most cost-effective and essential areas to focus security resources. Officials commented that prior Office of the Chief Information Officer leadership made the decision that contractor information would not be reported. However, officials indicated that reporting contractor information would be reassessed in the future.

Our review of the Department's third quarter FY 2015 FISMA submission also identified that contractor information had not been submitted for all Cross-Agency Priority (CAP) goals. Established by the *GPR Modernization Act of 2010*, the CAP goals are used to accelerate progress of presidential priority areas, such as cybersecurity, where implementation requires active collaboration between multiple agencies. The Department of Homeland Security identified several cybersecurity areas as CAP goals for FY 2015, including Information Security Continuous Monitoring, Identity Credential and Access Management, and Anti-Phishing and Malware Defense. In response to prior OIG evaluations, officials commented that reporting on all activities was critical to understanding the Department's cybersecurity posture. However, although Department officials indicated in response to our prior year report that performance metrics for both Federal and contractor resources would be reported in the future, we noted that none of the metrics related to identity credential and access management included contractor results. As a result, there was a lack of visibility into privileged or unprivileged account management within the Department and the number of users required to log onto the network using a two-factor Personal Identity Verification card.

Vulnerability Management

The Department made a number of improvements to its vulnerability management program since our prior evaluation. Specifically, the Department had taken action to correct four deficiencies identified in FY 2014 related to operating systems and/or applications that were running without current security patches for known vulnerabilities. However, our testing indicated that vulnerability management weaknesses continued to exist. Testwork at one location identified a number of systems that had not received antivirus updates in more than 30 days. Specifically, more than 1,300 laptops, workstations, and servers had not received antivirus signature definitions used to aid in the detection of viruses in a timely manner. Furthermore, although two locations addressed deficiencies noted in prior years, neither had fully implemented the patch/vulnerability management program as recommended, to include updating documentation, enhancing the vulnerability remediation process, and completing corrective action plans to validate, test, and verify the scanning process. Officials noted that plans were in place to address the weaknesses subsequent to our review.

In addition, several recent and/or ongoing reviews conducted by the OIG revealed issues related to the Department's vulnerability management program, such as the following:

- Our ongoing audit of a major Headquarters organization found numerous high and medium risk vulnerabilities on the entity's servers and workstations. For instance, we identified at least 80 workstations with high-risk vulnerabilities related to software such

as Web browsers and office automation products. Our testing also discovered more than 75 servers on the network that contained a server configuration vulnerability that was almost 10 years old. In addition, we identified a system that was using server management software that was no longer supported by the vendor.

- Our recently issued report on *Cybersecurity Controls Over a Major National Nuclear Security Administration System* (DOE/IG-0938, June 2015) identified a number of devices that had open ports or missing security patches, which increased the risk of insider threats to the system.
- Our ongoing audit of an Office of Science laboratory found several instances of systems with outdated antivirus software. In one case, the antivirus software of one system had not been updated in almost 8 months. Management indicated that the weaknesses existed on only a few of a large number of computers. We did not validate the size of the population at the site. However, without the latest updates, the systems were at risk of compromise by a virus or other destructive malware.

As noted in prior reports, the failure to apply patches and remediate vulnerabilities in a timely manner could result in unauthorized access to systems and information, as well as loss or disruption to critical operations. In addition, the Department's Office of Enterprise Assessments reported on vulnerability management weaknesses at numerous sites in FY 2015.

System Integrity of Web Applications

We identified weaknesses related to system integrity of Web applications at five locations. Our testwork revealed Web applications—including human resources, financial, and business applications—that did not properly validate input data, protect the confidentiality of user credentials, and/or analyze uploaded files, weaknesses that could result in unauthorized access to the application and compromise data reliability. Our evaluation found the following:

- Four applications accepted malicious input data that could be used to launch attacks against legitimate application users. Such attacks, known as cross-site scripting, could allow an attacker to gain unauthorized access to an application, make unauthorized changes to data, and disclose sensitive information.
- Six applications at four locations stored user authentication information in an unsecure manner on the network, making the authentication information accessible to any Web server on the same network. Under certain conditions, including if the other Web servers were under the control of a malicious actor, this insecure setting could have increased the risk of unauthorized access to and/or modification of sensitive information in Web applications.
- Applications at two locations allowed users to upload files without first scanning the files for malware. Web applications that do not properly analyze uploaded files are at risk for malicious attacks that could result in the distribution of a virus or other malware that could compromise application functionality and end-user workstations.

-
- While one location had made progress in addressing a prior year weakness, scheduled milestones for prioritizing Web servers for vulnerability scanning, remediating vulnerabilities, and using a risk acceptance process had not been completed at the time of our testwork.

Web applications that do not properly validate input data, such as those identified during our testing, are at risk for malicious attacks that could result in unauthorized access to application functionality and sensitive data stored in the application. Attackers could leverage Web application vulnerabilities to gain access to legitimate users' desktops or other key systems and applications on the internal network. The Office of Enterprise Assessments also reported on similar weaknesses related to system integrity of Web applications at several sites in FY 2015.

Access Controls and Segregation of Duties

Improvements in the Department's cybersecurity program related to account management resulted in the closure of eight prior year deficiencies. However, our current year testwork identified several new weaknesses in these areas:

- We identified a weakness related to the "least privilege principle" at one location. Specifically, 18 individuals were assigned responsibilities that could have allowed them to create profiles, assign profiles to others, and migrate data into production—privileges that were not necessary for job performance. Excessive privileges that are not necessary to perform assigned tasks increased the risk of unauthorized system configuration changes and user profile modifications.
- Another location did not always ensure that new users were aware of rules of behavior governing appropriate use of resources prior to granting system access. The rules of behavior addressed cybersecurity topics such as use of government equipment, incident handling and reporting, and password management.
- Our current evaluation also noted opportunities for improvement related to access controls and/or the segregation of duties at three sites. Specifically, we identified a failure to adequately manage user access privileges and perform periodic reviews of user accounts and segregation of duty conflicts. Absent effective account management practices, these weaknesses may increase the risk of unauthorized or malicious access to sensitive information systems and related applications.

Access control issues were also identified in our report on *Cybersecurity Controls Over a Major National Nuclear Security Administration System*. We noted that user passwords had not been regularly changed to reduce the risk of system compromise and ensure that users had been authorized to maintain access to the system. Similar to the issues we identified, the Office of Enterprise Assessments reported on access control deficiencies such as password weaknesses and inadequate management of privileged user accounts at a number of locations.

Cybersecurity Program Management

The weaknesses identified occurred, in part, because the Department had not ensured that policies and procedures were fully developed and/or implemented to meet all necessary cybersecurity requirements. In addition, the Department had not always implemented an effective performance monitoring and risk management program.

Policies and Procedures

The Department had not ensured that cybersecurity policies and procedures were developed and/or updated in a timely manner to provide assurance that information systems and data were adequately secured. As noted in our prior evaluation, the Office of Science had not updated its Program Cybersecurity Plan since June 2010 to reflect new cybersecurity risks and changes to national or Departmental policy. This issue was also noted in our ongoing audit of *The Department of Energy's Cybersecurity Risk Management Framework*, which found that the Office of Science's outdated cybersecurity plan had not established a process for sites to transition from a compliance-based cybersecurity program to a risk-based cybersecurity program. In addition, several issues identified during our FY 2015 review occurred because certain locations had not documented and implemented policies and procedures related to manual application security testing to supplement automated scanning, which could have assisted sites in identifying Web application vulnerabilities. We also noted that policies and procedures at one site did not clearly define user roles and responsibilities, which resulted in excessive privileges assigned to several application developers.

Even when policies and procedures were documented, they were not always fully implemented. Officials at one site had not fully implemented patch and vulnerability management policies and procedures to ensure that security patches were applied and that legitimate vulnerabilities were remediated in accordance with policy. Despite establishing requirements for managing the security of systems, applications, devices, and information, another location had not implemented secure coding practices to include encryption and other data protection controls during development of an in-house application. In addition, although one site had documented policies and procedures related to security training, processes were not followed related to requesting and retaining signed acknowledgements to ensure that all users were aware of and abided by rules of behavior governing cybersecurity topics.

Performance Monitoring and Risk Management

The Department had not implemented a fully effective performance monitoring and risk management program. Prior OIG reports have consistently noted problems with the Department's plan of action and milestones (POA&M) process, an important tool required to assist management in identifying, prioritizing, and tracking remediation activities for known cybersecurity weaknesses. While we noted that nearly all of the deficiencies identified during our FY 2014 evaluation were included in POA&Ms submitted to the Office of the Chief Information Officer, a significant improvement from prior years, we continued to identify concerns:

- We determined that the percentage of open milestones that were past the scheduled completion date were consistent with those identified during our FY 2014 evaluation.

Specifically, our analysis identified that 633 of 955 open milestones (66 percent) were overdue. Of those, 45 percent were at least 1 year beyond the estimated completion date.

- We noted an increase in the percentage of open weaknesses that had been assigned inadequate resources for remediation, as compared to our prior year's evaluation. Specifically, we determined that more than half of the Department's 665 open weaknesses had been assigned a cost of 1 dollar to remediate, a 10 percent increase over our FY 2014 evaluation. While we recognized that some weaknesses may have minimal costs for remediation, properly evaluating resources needed to mitigate a weakness is an important element that can be used by management in decision making related to prioritization of weakness remediation activities and budgeting for corrective actions.

We also found that risk management processes at locations reviewed were not always effective to identify and remediate cybersecurity weaknesses. In particular, many of the Web application vulnerabilities we identified occurred because effective processes had not been implemented to ensure that controls were in place to help identify and prevent application integrity weaknesses. For example, application development and vulnerability management programs at two sites did not include adequate testing and validation procedures to identify vulnerabilities related to input data validation safeguards. At two other locations, configuration settings had not been properly secured to protect user authentication information from potential compromise. We also determined that several sites reviewed had not implemented risk management processes to include the documentation and acceptance of the risks associated with Web application vulnerabilities.

In a number of instances, we found that a robust patch management program had not been implemented to effectively remediate vulnerabilities affecting operating systems and/or applications. An ineffective virus protection program at one location had not ensured that workstations, laptops, and servers were communicating properly and receiving necessary updates. Further, our ongoing audit of a Headquarters program found that personnel responsible for conducting security testing did not have the authority to remediate the vulnerabilities identified. Although vulnerability scan reports and results were shared with the appropriate offices for remediation, the weaknesses affecting both servers and workstations had not been fixed. In addition, we found that an Office of Science site's vulnerability management program did not include an aging process to track the time to patch and/or mitigate weaknesses, an important component of an effective risk management program and an area of focus included in FISMA reporting metrics developed by the Department of Homeland Security.

Risk to Information and Systems

Without improvements, such as adherence to policies and processes to ensure security controls are fully implemented, the Department's information and systems will continue to be at a higher-than-necessary risk of compromise, loss, and/or modification. The recent cybersecurity breach at the Office of Personnel Management, which affected more than 21 million Federal employees, contractors, applicants, and family members, further highlighted the importance of maintaining a robust cybersecurity posture. In addition, absent a fully effective process for tracking corrective actions using POA&Ms, the Department may not adequately address cybersecurity risks or

prioritize investments to ensure protection of data and information systems. In response to our report, management indicated that the existence of compensating controls reduced the likelihood of exploitation of identified vulnerabilities to a very low level. Although sites had implemented compensating controls to mitigate some of the identified weaknesses, our testwork found that the vulnerabilities identified during our FY 2015 evaluation could be exploited by a malicious insider and/or external attacker. As such, additional action is necessary to help strengthen the Department's unclassified cybersecurity program.

RECOMMENDATIONS

To improve the Department's unclassified cybersecurity program and to correct the weaknesses identified in this report, we recommend that the Administrator for the National Nuclear Security Administration, Under Secretary for Science and Energy, and Deputy Under Secretary for Management and Performance, in coordination with the Chief Information Officer, direct Federal and contractor programs and sites to:

1. Correct, through the implementation of appropriate controls, the weaknesses identified in this report;
2. Develop and implement policies and procedures, as needed, in accordance with Federal and Departmental requirements to ensure that systems and information are and remain adequately secured;
3. Ensure that effective performance monitoring and risk management practices are implemented, to include fully developing and utilizing PO&AMs to track and prioritize remediation of all cybersecurity weaknesses requiring corrective actions; and
4. Include complete information for both Federal and contractor-managed cybersecurity programs when reporting annual and quarterly performance metrics to the Department of Homeland Security.

MANAGEMENT RESPONSE

Management concurred with each of the report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report. For instance, management stated that weaknesses identified in our report would be recorded and tracked through the Department's POA&M process. In addition, the Office of the Chief Information Officer stated that it will enhance validation and assessment capabilities to assist in the management of POA&Ms at the organizational and program office levels. Management also indicated that it would continue to deploy its Information Security Continuous Monitoring Strategy in an effort to gather performance data and essential, near real-time cybersecurity information. Furthermore, management commented that it would continue to work to identify an effective means to capture performance metrics data for all Department entities and to gather more accurate, complete information for FISMA metric areas, particularly those related to CAP goals.

AUDITOR COMMENTS

Management's comments and planned corrective actions 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 (Department) unclassified cybersecurity program adequately protected its data and information systems.

Scope

We conducted the evaluation from February to November 2015 at 22 Department locations under the responsibility of the Administrator, National Nuclear Security Administration, Under Secretary for Science and Energy, Under Secretary for Management and Performance, and the Administrator, Energy Information Administration. The focus of our evaluation was the Department's unclassified cybersecurity 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 review did not include a determination of whether the vulnerabilities were actually exploited. While we did not test every possible exploit scenario, we did conduct testing of various attack vectors to determine the potential for exploitation. This report also considers the results of other reviews conducted by the Office of Inspector General related to the Department's cybersecurity program. This evaluation was conducted under Office of Inspector General project number A15TG020.

Methodology

To accomplish our objective, we:

- Reviewed Federal regulations and Department directives pertaining to information and cybersecurity.
- 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 cybersecurity-related functions, such as cybersecurity plans and plans of action and milestones.
- 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 the Office of Inspector General's contract auditor, KPMG LLP (KPMG). Office of Inspector General and KPMG work included analysis and testing of general and application controls for systems, as well as internal and external vulnerability testing of networks, systems, and workstations. In utilizing the work of KPMG, we performed procedures that provided a sufficient basis for the use of that work, including obtaining evidence concerning the auditors' qualifications and independence, and reviewing the work to determine that the scope, quality, and timing of the work performed was adequate for reliance in the context of our evaluation objectives.
- Evaluated and incorporated the results of other cybersecurity review work performed by the Office of Inspector General, the Government Accountability Office, and the Office of Enterprise Assessments' Office of Cyber and Security Assessments.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objective. Accordingly, we assessed significant internal controls and the Department's implementation of the *GPRA Modernization Act of 2010* and determined that it had established performance measures for its information and cybersecurity program. Because our review 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 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.

Because of the size and complexity of the Department's enterprise, it is virtually impossible to conduct a complete, comprehensive assessment of each site and organization each fiscal year. As such and as permitted by FISMA, we utilized a variety of techniques and leveraged work performed by other oversight organizations to form an overall conclusion regarding the Department's cybersecurity posture. This report describes a number of specific problems that, in our view, should be addressed by responsible officials to improve the overall cybersecurity posture of the Department. Because of the non-homogeneous nature of the population, users of this report are advised that testing during this evaluation was based on judgmental system selections and as such, the weaknesses discovered at certain sites may not be representative of the Department's enterprise as a whole.

Management waived an exit conference.

RELATED REPORTS

Office of Inspector General

- Audit Report on [*Cybersecurity Controls Over a Major National Nuclear Security Administration Information System*](#) (DOE/IG-0938, June 2015). Our audit revealed that the cybersecurity controls for a major information system at the National Nuclear Security Administration had not been adequately developed, documented, or implemented. Specifically, we identified weaknesses related to the implementation of access controls and the development and implementation of effective database change management, configuration management, and continuous monitoring processes. The weaknesses identified occurred, in part, because site officials did not ensure that Federal security requirements were fully implemented. In addition, site officials had not established a formal service level agreement with the system's vendor to define ongoing support requirements for the system.
- Evaluation Report on [*The Department of Energy's Unclassified Cybersecurity Program – 2014*](#) (DOE/IG-0925, October 2014). The Department of Energy (Department) had taken positive actions to improve the security and awareness of the unclassified cybersecurity program. While the Department made strides to correct previously identified deficiencies, additional effort is needed to ensure that the risk of operating systems are identified and that systems and information are adequately secured. In particular, our fiscal year (FY) 2014 evaluation identified weaknesses related to performance metric reporting, patch and configuration management processes, access controls, and system integrity of Web applications. The issues occurred, at least in part, because the Department's programs and sites had not ensured that cybersecurity policies and procedures were developed and properly implemented. In addition, the Department's performance monitoring and risk management programs were not completely effective.
- Special Report on [*Management Challenges at the Department of Energy – Fiscal Year 2015*](#) (DOE/IG-0924, October 2014). Based on the work performed during FY 2014, the Office of Inspector General identified six areas, including cybersecurity, which remained a management challenge for FY 2015.
- Audit Report on [*The Department of Energy's Implementation of Voice over Internet Protocol Telecommunications Networks*](#) (DOE/IG-0915, June 2014). Our review identified opportunities to improve the efficiency and enhance cybersecurity of the Department's Voice over Internet Protocol (VoIP) networks. In particular, we found that programs and sites had not always applied required cybersecurity controls to VoIP networks, thus increasing the risk of compromise. The issues identified occurred, in part, because the Department had not adequately monitored the implementation of cybersecurity controls for VoIP systems. Without improvements, the duplicative and fragmented VoIP implementation approach that we identified could continue unabated and result in additional, unnecessary expenditures of resources at programs and/or sites that have not yet upgraded to VoIP systems.

- Special Report on the [*Office of Energy Efficiency and Renewable Energy's Integrated Resource and Information System*](#) (DOE/IG-0905, April 2014). Our review largely substantiated the allegations received related to contract and project management. We discovered that the Office of Energy Efficiency and Renewable Energy (EERE) had not effectively managed the development and implementation of the Integrated Resource and Information System (IRIS). In particular, EERE failed to follow the Department's structured capital planning and investment control process and had not provided effective monitoring of the project. In addition, EERE had not implemented key cybersecurity controls designed to protect IRIS and the network on which it resided. Without a well-defined project planning and execution process that includes baselines and deliverables, EERE could not ensure that significant funds spent on IRIS and other future information technology projects were used in a cost-effective manner.
- Special Report on [*The Department of Energy's July 2013 Cyber Security Breach*](#) (DOE/IG-0900, December 2013). In spite of a number of early warning signs that certain personnel-related information systems were at risk, the Department had not taken action necessary to protect the personally identifiable information of a large number of its past and present employees, their dependents, and many contractors. We concluded that the July 2013 incident resulted in the exfiltration of a variety of personally identifiable information on over 104,000 individuals. Our review identified a number of technical and management issues that contributed to an environment in which this breach was possible. Compliance and technical problems included the frequent use of complete social security numbers as identifiers, permitting direct Internet access to a highly sensitive system without adequate security controls, lack of assurance that required security planning and testing activities were conducted, and failure to assign the appropriate level of urgency to replace end-of-life systems. We also identified numerous contributing factors related to inadequate management processes. These issues created an environment in which the cybersecurity weaknesses we observed could go undetected and/or uncorrected. While we did not identify a single point of failure that led to the breach, the combination of the technical and managerial problems we observed set the stage for individuals with malicious intent to access the system with what appeared to be relative ease.
- Special Report on [*Management Challenges at the Department of Energy – Fiscal Year 2014*](#) (DOE/IG-0899, November 2013). Based on the work performed during FY 2013, the Office of Inspector General identified eight areas, including cybersecurity, which remained a management challenge for the Department in FY 2014.
- Evaluation Report on [*The Department of Energy's Unclassified Cyber Security Program – 2013*](#) (DOE/IG-0897, October 2013). The Department had taken a number of positive steps over the past year to correct cybersecurity weaknesses related to its unclassified information systems. 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. 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. 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 cybersecurity requirements. In addition, the Department continued to operate a less than fully effective performance monitoring and risk management program. Absent improvements to its unclassified cybersecurity program, the Department's information and systems will continue to be at a higher-than-necessary risk of compromise.

- Audit Report on [*Management of Naval Reactors' Cyber Security Program*](#) (DOE/IG-0884, April 2013). Although the Naval Reactors Program had made a number of enhancements to its cybersecurity 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 weaknesses identified occurred, in part, because officials had not ensured that necessary cybersecurity controls were fully implemented. Specifically, they had not fully developed and/or implemented policies and procedures related to vulnerability management, access controls, incident response, and cybersecurity training. In addition, Naval Reactors had not always effectively used plans of action and milestones to track, prioritize, and remediate cybersecurity weaknesses.
- Audit Report on [*Management of Los Alamos National Laboratory's Cyber Security Program*](#) (DOE/IG-0880, February 2013). Los Alamos National Laboratory (LANL) had taken steps to address concerns regarding its cybersecurity program raised in prior evaluations. However, we identified continuing concerns related to LANL's 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 LANL's cybersecurity 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 LANL's Information Technology Directorate had not followed National Nuclear Security Administration policies and guidance for assessing system risk and had not fully implemented LANL's own policy related to ensuring that scanning was conducted to identify and mitigate security vulnerabilities in a timely manner.

Government Accountability Office

- [*FEDERAL INFORMATION SECURITY: Agencies Need to Correct Weaknesses and Fully Implement Security Programs*](#) (GAO-15-714, September 2015)
- [*INFORMATION SECURITY: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies*](#) (GAO-15-758T, July 2015)
- [*CYBERSECURITY: Actions Needed to Address Challenges Facing Federal Systems*](#) (GAO-15-573T, April 2015)

- [*INFORMATION SECURITY: Agencies Need to Improve Oversight of Contractor Controls*](#) (GAO-14-612, August 2014)
- [*CYBERSECURITY: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies*](#) (GAO-15-725T, June 2014)
- [*INFORMATION SECURITY: Federal Agencies Need to Enhance Responses to Data Breaches*](#) (GAO-14-487T, April 2014)
- [*INFORMATION SECURITY: Agencies Need to Improve Cyber Incident Response Practices*](#) (GAO-14-354, April 2014)
- [*FEDERAL INFORMATION SECURITY: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness*](#) (GAO-13-776, September 2013)
- [*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)


MANAGEMENT COMMENTS



Department of Energy
Washington, DC 20585

October 23, 2015

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

FROM: MICHAEL M. JOHNSON 
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General's Draft Report on "The Department's
Unclassified Cyber Security Program – 2015"

Thank you for the opportunity to comment on the Draft Evaluation Report, "The Department's Unclassified Cyber Security Program - 2015." Despite significant improvements in the cybersecurity posture of the Department, cyber-attacks from highly-capable, malicious actors continue to increase in their complexity, frequency, and aggression. The known areas of weakness must continue to be addressed at an Enterprise level to ensure that Department of Energy (DOE) information assets and systems are adequately protected from harm. For these reasons, the Office of the Chief Information Officer (OCIO) is addressing enterprise cybersecurity through a collaboratively developed DOE Cyber Strategy. The Strategy is founded on the management of information as a Department asset and the use of a distributed standards-based, shared-risk management approach that provides for secure sharing of information.

The specific assessments in this report will assist the OCIO and Program Offices in determining appropriate follow-up actions to resolve specific findings and to improve the cybersecurity program as a whole. In regards to the specific recommendations in this draft report, the Department responds as follows.

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 Program in a Plan of Action and Milestone (POA&Ms) report. The responsible Program will provide specific actions to address the open findings and report against the estimated weakness completion dates and corrective actions through quarterly POA&M reporting. The DOE OCIO will confirm that weaknesses noted in this report are recorded and tracked as POA&Ms. OCIO anticipates that the Programs will begin reporting on these findings in their first quarter fiscal year (FY) 2016 report. The OCIO will also include applicable findings in its program-level POA&M report for first quarter FY 2016.

These issues will be addressed by and in accordance with the timelines mitigating the weaknesses identified in this report and already approved by National Nuclear Security Administration (NNSA) and the Office of the Inspector General (OIG).

Estimated Completion Date: December 31st, 2015

Recommendation 2. *Develop and implement policies and procedures, as needed, in accordance with Federal and Department requirements to ensure systems and information are and remain adequately secured.*

Response: Concur.

DOE Order (O) 205.1B, Change 3, *The Department of Energy Cyber Security Program*, describes the requirements for the Department's cybersecurity program. The current Order includes requirements related to the implementation of controls from publications of the National Institute of Standards and Technology and the Committee on National Security Systems that are to be cascaded through the Department in Program Risk Management Implementation Plans (RMIPs). Previous revisions to the Order added requirements for the complete documentation of security requirements in information technology acquisitions and for the development and documentation of Program Office supply chain risk management processes.

An initiative to update the Order, including the documentation of incident management processes, began late in the fourth quarter FY 2015. A working group under the DOE Information Management Governance Board will review the current Order and determine a collaborative approach to its update to include more standards-based guidance for implementing security policies. The Office of Information Technology Policy & Governance (IM-20) will coordinate the revision of this Order.

NNSA will collaborate with the Department as appropriate to address the recommendations and address any policy and procedures changes that DOE will implement.

Estimated Completion Date: March 31st, 2016

Recommendation 3. *Ensure that effective performance monitoring and risk management practices are implemented, to include fully developing and utilizing POA&Ms to track and prioritize remediation of all cybersecurity weaknesses requiring corrective actions.*

Response: Concur.

The Program Offices monitor POA&Ms for all subordinate organizations through internal processes that are to be documented in RMIPs per DOE O 205.1B. The POA&Ms are part of contractor assurance systems used to assess whether risk is being identified and

mitigated to an acceptable level in accordance with the mission. The DOE OCIO is enhancing its capability to assist in managing POA&Ms at the organizational and Program Office levels. Enhanced OCIO validation and assessment capabilities for POA&Ms and the Enterprise Cyber Governance System (ECGS), which allows for real-time update to POA&M status as well as a centralized repository for cybersecurity weakness remediation activities, provides tools that Program Offices can use to identify weaknesses, better manage remediation activities, and prioritize actions. Programs will manage progress and completion of POA&Ms and report quarterly to the DOE OCIO.

A key part of performance management includes the use of standard tools to improve continuous monitoring, risk management, and information sharing. Continued deployment of the DOE Information Security Continuous Monitoring (ISCM) Strategy will provide additional feedback into performance and implementation of security and risk management processes. In close coordination with the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) initiative, the ISCM Strategy provides capabilities to gather performance data and essential, near real-time cybersecurity status. OCIO will continue to expand the use of CDM tools and technologies across sites and Programs to provide data to a Departmental dashboard of cybersecurity performance.

NNSA technologies are being implemented to more effectively meet the DOE IG recommendations. The use of these technologies has progressed with full functionality planned for as resources are available. The infrastructure that employs these governance, risk, and compliance technologies are implemented using a modular approach to include more real time POA&M management.

Estimated Completion Date: September 30th, 2016

Recommendation 4. *Include complete information for both Federal and contractor managed cybersecurity programs when reporting the status of performance metrics annually to the Department of Homeland Security.*

Response: Concur.

Reporting Federal Information Security Modernization Act (FISMA) metrics for Departmental activities, including those of the National Laboratories, is critical to a complete understanding of the Department's Cybersecurity posture. The OCIO will continue to work with the Programs to identify effective means to capture performance metrics data for all Departmental entities. OCIO will ensure that a strategy is implemented to gather more accurate, complete data for FISMA metrics and particularly relative to the Cross-Agency Priority goals. New efforts are underway in the OCIO to consolidate data collection efforts and provide more data on Departmental activities through all reporting requirements. The FY16 annual FISMA report will be completed and submitted by the OMB-required due date.

NNSA comprehensively reports required FISMA data as prescribed by OMB and DHS guidance to DOE OCIO. NNSA considers this item closed.

Estimated Completion Date: September 30th, 2016

If you have any questions or need additional information, please contact Mr. Robert Ciochon, Acting Associate Chief Information Officer for Cybersecurity, at 202-586-0166.

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.