U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

EVALUATION REPORT

The Department of Energy's Unclassified Cybersecurity Program – 2014

DOE/IG-0925

October 2014

Department of Energy
Washington, DC 20585

October 22, 2014

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department of Energy's Unclassified Cybersecurity Program – 2014"

BACKGROUND

The use of information technology by Federal entities is evolving rapidly, leading to advancements in areas such as virtualization technologies, cloud computing, and mobile devices that offer opportunities to increase the value and accessibility of Government resources and information. However, this progression also exposes Federal information and systems to new and constantly changing threats. In its Fiscal Year (FY) 2013 report to Congress, the Office of Management and Budget reported that the volume and sophistication of attacks against Federal resources continued to grow, increasing by approximately 26 percent over those reported in FY 2012. As such, it is important that the Federal government, to include the Department of Energy, reduce its information security risks to a level commensurate with the criticality of its systems and the sensitivity of the information within them.

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. In addition, Federal agencies are required to provide acceptable levels of security for the information and systems that support their operations and assets. Further, FISMA mandated that agency Offices of Inspector General conduct annual independent evaluations to determine whether agencies' unclassified cybersecurity programs adequately protected unclassified data and information systems. This report documents the results of our evaluation for the Department for FY 2014.

RESULTS OF EVALUATION

During FY 2014, the Department, including the National Nuclear Security Administration, had taken positive actions to improve the security and awareness of the unclassified cybersecurity program. While the Department continued to make progress in correcting deficiencies identified in prior years, additional effort is needed to ensure that the risks of operating systems are identified and that systems and information are adequately secured. In particular:

- Even though contractor resources accounted for a majority of the Department's more than 500 systems, it still had not reported performance metric data for all contractor systems. In response to our prior year's evaluation, management indicated its intent to fully report metrics for all contractor systems. However, we found that a significant percentage of the metric information reported to the Department of Homeland Security as part of annual FISMA reporting requirements excluded contractor systems.

- We discovered network systems and workstations at 13 locations with patch management weaknesses of varying degrees of criticality. Specifically, critical and high-risk vulnerabilities were identified on many of the systems and networks tested.

- Our testing also revealed that six locations had weaknesses related to system integrity of Web applications. In these instances, Web applications—including business, human resources, and general support applications—did not properly validate input data, increasing the risk of malicious attacks that could result in unauthorized access to the application and sensitive data stored within them.

- At eight locations, issues related to weaknesses in logical access controls were identified that could allow an attacker to gain access to sensitive data or disrupt network connectivity to systems, applications, and devices.

- Weaknesses related to the configuration management process, including inadequate support for testing and approving changes, existed at four locations. Configuration management involves the identification and management of security features for all components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle.

- At three locations, the overall security management program contained various deficiencies related to cybersecurity training, audit logging and monitoring, system inventories, incident reporting, and contingency planning.

The issues identified occurred, at least in part, because the Department's programs and sites reviewed had not ensured that cybersecurity policies and procedures were developed and properly implemented. For example, numerous locations had not implemented processes that could have prevented many of the weaknesses identified during our testing. In addition, as noted in our prior evaluation report, the Department's performance monitoring and risk management programs were not completely effective.

Without improvements, the Department's unclassified cybersecurity program will continue to operate at a higher-than-necessary level of risk. In addition, the weaknesses identified in this report should be thoroughly considered as the Department transitions its cybersecurity program from the traditional compliance-based process to one that supports the National Institute of Standards and Technology's Risk Management Framework and continuous system authorizations. Continued deficiencies in the areas outlined in this report could adversely affect the Department's ability to gain or retain assurance that its systems and data are operated and maintained within acceptable levels of risk.

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 sites and, in many cases, initiated corrective actions to address the identified deficiencies.

MANAGEMENT REACTION

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 their entirety in Appendix 3.

Attachment

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

EVALUATION REPORT ON THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2014

TABLE OF CONTENTS

Evaluation Report

Details of Finding 1

Recommendations 9

Management Response and Auditor Comments 10

Appendices

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

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2014

DETAILS OF FINDING

The *Federal Information Security Management Act of 2002* (FISMA) mandated that agency Offices of Inspector General conduct annual independent evaluations to determine whether unclassified cybersecurity programs adequately protected data and information systems. During Fiscal Year (FY) 2014, we reviewed the unclassified cybersecurity programs at 24 Department of Energy (Department) locations, including Headquarters. The scope of our fieldwork activities included validating corrective actions taken to remediate prior year weaknesses, reviewing information technology controls over networks and applications, and conducting technical vulnerability scanning both within and external to the networks.

Actions taken to improve the Department's unclassified cybersecurity program since our prior evaluation resulted in the closure of 25 of the 39 deficiencies reported in our FY 2013 review. However, test work performed in conjunction with the current year's review continued to identify weaknesses in the same areas reported in past years. Specifically, our review of the Department's Under Secretary for Nuclear Security, Under Secretary for Science and Energy, and Under Secretary for Management and Performance organizations found that additional effort is needed to ensure that systems and information are adequately secured, and the risks of operating systems are known. Based on the results of our FY 2014 evaluation, we identified vulnerabilities at many of the 24 locations reviewed, including 11 new and 14 unresolved weaknesses from prior years' reviews.

Program Improvements

During FY 2014, the Department, including the National Nuclear Security Administration (NNSA), had taken several positive actions to improve the security and awareness of its unclassified cybersecurity program. In particular:

- In July 2014, the Department's Cyber Council formalized and approved its *Information Management Governance Framework*. The overall goals of the framework are to support mission enhancement, operational excellence and risk management across the Department. It is intended to ensure that policy decisions are appropriate, foster open and honest communication, and support collaborative oversight of information management to achieve transparency and accountability.

- NNSA continued to enhance its Enterprise Continuous Monitoring Program. When fully implemented, this automated solution is expected to enable the transformation of the static compliance-based risk determination process into a dynamic process, thus facilitating near real-time situational awareness and appropriate cost-effective risk-based decisions. As of August 2014, NNSA reported that all of its sites, including Headquarters, had successfully established and were operating internal data feeds supporting information related to systems, FISMA compliance and plan of action and milestone progress.

- The Office of Environmental Management continued to implement its Mission Information Protection Program, which provided enterprise capabilities to 15 sites through its Continuous Monitoring Center. Program capabilities included firewalls, capture of network traffic, intrusion detection, malware reverse engineering, vulnerability scanning, log management, patching of third-party products and other custom solutions that provided additional insight into the Office of Environmental Management's cybersecurity posture.

- The Office of the Chief Information Officer reported various cybersecurity improvements that resulted in significant risk reduction to the operating environment it manages. As of July 2014, officials reported that the organization had implemented configuration enhancements to its architecture and operating environment, deployed a virtual desktop infrastructure service, reduced the number of critical systems with Internet access, added risk mitigation capabilities to its servers and gateway, and improved vulnerability and patch management processes and procedures.

Although these actions should help improve enterprise-level awareness and management of the Department's unclassified cybersecurity program, our current evaluation identified weaknesses that, if left uncorrected, could adversely affect the Department's ability to identify, assess, and mitigate new and existing threats and risks to its systems and data.

Unclassified Cybersecurity Program Implementation

The FY 2014 evaluation identified an ongoing area of concern related to the completeness of cybersecurity performance metrics reported to the Department of Homeland Security (DHS) for analysis and consideration in the Office of Management and Budget's annual FISMA report to Congress. In addition, our current evaluation identified weaknesses in security patch management, system integrity of Web applications, access control, configuration management, and security management. Taking into consideration the Department's risk-based approach to cybersecurity, the weaknesses noted in our report generally had not been identified and/or the risk posed by the weaknesses accepted by management prior to our testing.

Security Reporting

Contrary to management comments on our prior year's evaluation, the Department still had not reported performance metric data for all contractor systems. Performance metrics related to 11 cybersecurity areas are to be reported to DHS and the Office of Management and Budget under the requirements of FISMA. The failure to report contractor system information was first identified in our evaluation report on *The Department of Energy's Unclassified Cyber Security Program – 2013* (IG-0897, October 2013). In response, management stated that performance metrics would be reported for both Federal and contractor resources. However, our review of the FY 2013 annual report submitted to DHS found that 60 of 97 metrics requested had been completed for Federal systems only, even though contractor resources accounted for 359 of the Department's 511 (70 percent) reported systems. As a result, the Department did not provide complete information related to its cybersecurity program in all or a portion of eight reporting areas, including configuration management, vulnerability and weakness management, identity and access management, boundary protection, and remote access. In addition, representatives

from a number of locations indicated that information related to the *Administration Priority* topics (continuous monitoring, identity management, and boundary protection) was either not applicable or had not been requested by the cognizant Headquarters element. As such, progress towards implementing important initiatives such as *Homeland Security Presidential Directive 12*, could not be effectively measured.

Our review of the Department's data call for the FY 2014 annual FISMA report to DHS found that contractor results still had not been requested for metrics related to data protection and incident management, and only partial results had been requested for metrics related to asset management, identity and access management, remote access, and boundary protection. While the Department's Memorandum of Understanding with DHS allowed for documented, mutually acceptable alternative methodologies, such action had not been taken to modify the Department's reporting requirements.

Patch Management

The Department continued to make improvements to its patch management program, resulting in the closure of four prior-year deficiencies in this area. However, our testing of a limited number of network segments, general business and related systems, and workstations at 13 locations identified weaknesses of varying degrees of criticality. Specifically, critical and/or high-risk vulnerabilities were identified on many of the systems and networks tested. For instance:

- One location was running operating system and/or client applications without current security patches for known vulnerabilities that had been released more than 90 days prior for 235 of 270 (87 percent) workstations tested. Missing patches included those for productivity, mobile device management and remote access applications, databases, development environments, media players, and Web browser add-ons. Similarly, another location had not completed corrective action to correct the weaknesses identified during our prior year's evaluation.

- Network systems at three locations were running operating system and/or application software without current security patches for known vulnerabilities that had been released more than 30 days prior to testing. Similar issues had been noted at two of these locations for at least 4 years. Overall, we identified 180 instances of outdated or missing patches on these systems.

- Two locations were running operating systems or applications that were no longer supported by the vendor on 16 servers—2 of which had not been supported since 2010. In addition, two systems at one location were using an application for which vendor support had ended in late 2013. In this case, management indicated that the upgrade to a supported application was planned to be completed in late 2014. However, until such action is completed, the risk to the systems and information remains higher than necessary. This issue is similar to weaknesses identified in our Special Report on *The Department of Energy's July 2013 Cyber Security Breach* (DOE/IG-0900, December 2013).

Although officials at the reviewed locations noted that certain controls to mitigate the risks associated with these security weaknesses had been implemented, an attacker may have been able to successfully execute attacks against the vulnerable servers, applications, and workstations by using publicly available exploits as well as custom attacks with no known signatures. Exploitation by unauthorized or malicious individuals could lead to disruption of sensitive data or systems, as well as theft or improper disclosure of confidential business information. Notably, the Department's Office of Enterprise Assessments reported similar issues at four locations in FY 2014.

System Integrity of Web Applications

We identified numerous weaknesses at six locations related to system integrity of Web applications. In these instances, Web applications—including business, human resources, and general support applications—did not properly validate input data, increasing the risk of malicious attacks that could result in unauthorized access to the application and sensitive data stored within them. Specifically:

- Twelve applications at six locations accepted malicious input data that could be used to launch attacks to gain unauthorized access to the application. Such attacks, known as cross-site scripting, could allow an attacker to compromise legitimate users' workstation and application logon credentials. One of the 10 applications also did not validate input data and allowed the data to be used in improperly designed queries, thereby making the application vulnerable to attacks against the application's database server. This type of attack could result in the loss or modification of information stored within the database.

- Another application used to support financial processing did not properly validate access privileges associated with end-user requests. We found that the application could accept requests regardless of the role the requesting user had been assigned and could have allowed unauthorized access to the system's information.

- One access control application stored user authentication information in an unsecured manner on the system, making the information accessible to any Web server on the same network. Web applications that do not properly protect the confidentiality of user authentication tokens are at increased risk of unauthorized access to the application and sensitive data stored within the system.

- One location had corrected specific issues identified in prior years. However, its corrective action plan to implement Web access management and user identity administration functionality and develop a risk-based approach for managing its Web applications had not been completed.

Web application attacks could have negative impacts on the security of the information systems, as well as application and data reliability. The Office of Enterprise Assessments noted similar issues at five locations it reported on in FY 2014.

Access Control

Although the Department had taken steps to correct several of the access control-related weaknesses identified in our prior year's review, several locations continued to experience problems in this area. Strong access controls provide assurance that access to information technology resources is reasonable and restricted to authorized individuals. Our review found:

- Eight locations had not performed a periodic review of system accounts and/or disabled or removed system accounts in a timely manner. For instance, two locations had not completed actions to correct issues identified during our previous evaluation. Another location conducted a management review of user accounts to identify and remove those that were associated with terminated employees. However, the review was performed using an outdated database and, as a result, officials still had not disabled or removed terminated users' access in a timely manner. Although required by site-level procedures, a fourth location had not deactivated seven user accounts in a timely manner upon termination, including three that were not set to expire after 60 days of inactivity.

- Three locations had not securely configured network servers, devices and/or workstations to protect against unauthorized access. We identified 41 servers, 14 workstations and 2 network devices that were configured with default or easily guessed passwords. In addition, two file shares, five servers and one network device at two of the locations were configured to allow connections from any other system without the use of authentication or other access controls. Further, numerous systems at one location were affected by an authentication bypass vulnerability that could allow an individual to logon as an administrator without a password.

Databases with default or weak login credentials are at increased risk of unauthorized access, which could allow an attacker to gain access to sensitive data. Unauthorized access to network devices could result in a disruption of network connectivity to those devices or even unauthorized access to other key systems, applications and devices. The Office of Enterprise Assessments also identified similar weaknesses at five locations in FY 2014.

Configuration Management

Our evaluation identified weaknesses related to the configuration management process at four locations. Configuration management involves the identification and management of security features for all components of an information system at a given point and systematically controls changes to that configuration during the system's life cycle. At one location, although modifications to the property management application were tracked, our review of a sample of changes found that change requests did not contain sufficient details to determine whether the changes had been authorized, tested and approved prior to implementation.

In addition, changes made to applications at three locations had been performed by developers without appropriate segregation of duties, including providing developers with administrator access to the application's production environment even though such privilege was not needed to perform their job functions. At another location, we found that previously identified weaknesses

related to the application change control process still had not been fully remediated. In several instances, management indicated that mitigating controls were in place, and the risk of the identified weaknesses had been accepted.

Security Management

Our evaluation identified several weaknesses at one location related to the site's overall security management program. In particular, site officials had not ensured that personnel with information security responsibilities had received specialized, role-based training, system access and activity was not logged and monitored, and servers and the information supporting the logging and security functions were not always protected from unauthorized access, modification and/or deletion. In addition, the site had not developed a complete inventory of information system assets, and all lost/stolen equipment was not appropriately reported to the Department's Joint Cybersecurity Coordination Center. Although these weaknesses had been discovered during our prior year's evaluation, the site had not completed corrective actions in these areas. Management indicated that remediation was expected to be completed in FY 2015.

The evaluation also identified opportunities for improvement related to contingency planning at two locations. One location had not reviewed and updated its Continuity of Operations and Information Technology Disaster Recovery Plans in almost 3 years, despite the requirements to do so at least annually. In addition, although one site was preparing its Business Impact Analysis at the time of our testing, the document had not been completed. The Office of Enterprise Assessments identified similar issues related to training, incident response, contingency planning and/or audit logging processes within the unclassified cybersecurity programs at all locations reported on during FY 2014.

Management of the Unclassified Cybersecurity Program

The issues identified occurred, at least in part, because the Department's elements had not ensured that cybersecurity policies and procedures were developed and implemented. In addition, as noted in our prior evaluation report, the Department continued to encounter weaknesses related to effective performance monitoring and risk management programs.

Policies and Procedures

The Department's programs had not always established or updated cybersecurity policies in a timely manner to ensure that site systems were not exposed to a higher than necessary level of risk. In particular, despite noting that it would be updated at least every 2 years, the Office of Science had not updated its *Program Cybersecurity Plan* since June 2010. This policy is meant to provide a foundation for ensuring the confidentiality, integrity and availability of information and systems at the National Laboratories managed by the Office of Science. However, a review of the current plan noted that, in at least one instance, it required the use of an outdated version of cybersecurity requirements promulgated by the National Institute for Standards and Technology. Officials within the Office of Science indicated that the plan was expected to be at least partially updated by December 2014.

In addition, several issues identified during the FY 2014 evaluation occurred because sites had not documented processes and procedures to ensure that unclassified cybersecurity programs adequately protected the sites' unclassified systems and information. Specifically, two locations had not fully established procedures to ensure security vulnerabilities were identified, monitored and remediated in a timely manner, including weaknesses related to default and easily guessed passwords. In addition, four locations had not developed processes to validate input information and/or identify, monitor and remediate vulnerabilities in Web-facing applications, and one location had not developed procedures to establish auditable events and audit record retention periods.

Although processes and procedures at certain locations had been documented, they were not always fully implemented. In one case, we found that system security officials were unaware of the process requirements. In addition, while processes had been developed and implemented at three locations, the processes did not always work as expected. For example, one site had implemented a system to block vulnerable hosts from connecting to the network; however, coding errors within the system prevented it from initiating blocks in some cases. At another location, system changes had not been fully tested to ensure that they had not negatively affected the system's functionality.

Performance Monitoring and Risk Management

Since our prior review, the Department had made limited progress in improving its corrective action tracking process. Specifically, the use of plans of action and milestones is required to identify and measure progress toward remediating known cybersecurity weaknesses. When used properly, the process can be an invaluable monitoring tool for management to identify, prioritize and track remediation activities for known cybersecurity weaknesses. However, we identified concerns that hampered management's ability to use the tool as envisioned. In particular:

- Although all programs submitted plans of action and milestones to the Department's Office of the Chief Information Officer, they were not always complete and, as such, did not provide a complete inventory of known weaknesses. We found that 22 of 39 weaknesses identified during our FY 2013 evaluation were not tracked in the plans of action and milestones submitted to the Department. As noted in our prior reports, failure to track and report known weaknesses deprives senior Department management of needed visibility into critical weaknesses in the unclassified cybersecurity program.

- Similar to our FY 2013 evaluation, we noted that the percentage of overdue milestones continued to increase. We found that 699 of 1,072 (65 percent) open milestones were past the scheduled completion date—a significant increase from the 51 percent reported in the prior year. Of those, almost half had exceeded their expected completion date by more than a year. While it is not expected that all corrective actions would be completed as scheduled, the increase in the number of missed milestones concerns us.

- Our analysis determined that 266 of the Department's 638 (42 percent) open weaknesses had been assigned a remediation cost of 1 dollar. The required resources are an

important element used by management in prioritizing and budgeting for corrective actions. Interestingly, weaknesses assigned to the Office of the Chief Information Officer accounted for more than half of these items.

- In many cases, the Department's plans of action and milestones did not provide information at a level of granularity that would allow management to monitor and track progress made toward remediating weaknesses. Specifically, approximately two-thirds of open weaknesses only had one associated milestone.

Several locations had not implemented risk management programs that allowed the Authorizing Official[1] to fully consider all risks when accepting the risk of system operation. For example, at two locations, the risk management process did not include documentation and acceptance of risks related to operating Web applications. Another location had not fully implemented its risk management program to include an accurate system inventory, which could increase the risk of implementing inadequate security controls on systems.

Risk to Information and Systems

Without improvements, the Department's unclassified cybersecurity program will continue to operate at a higher-than-necessary level of risk. Deficiencies in developing, updating and implementing guidance and processes have adversely affected the Department's ability to properly secure its systems and the information stored within them. In addition, the weaknesses identified throughout this report may increase the risk of unauthorized disclosure of sensitive information in mission-based and financial systems and, as such, should continue to be addressed by management. Further, ineffective tracking of known cybersecurity weaknesses could result in understating a system's residual risk—that risk remaining after mitigation of known weaknesses—resulting in the Authorizing Official assuming responsibility for the system without having full awareness of its vulnerabilities.

The weaknesses identified in this report should be thoroughly considered as the Department transitions its cybersecurity program from the traditional compliance-based certification and accreditation process to one that supports the National Institute of Standards and Technology's Risk Management Framework and ongoing system authorizations. Without improvements in the areas listed within this report, the Department's ability to gain or retain assurance that its systems and data are operated and maintained within tolerable levels of risk could be adversely affected.

[1] An Authorizing Official is a senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk.

RECOMMENDATIONS

To improve the Department's unclassified cybersecurity program and to correct the weaknesses identified in this report, we recommend that the Under Secretary for 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, direct Federal and contractor programs and sites to:

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

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

3. Fully develop and utilize plans of action and milestones to improve its performance monitoring program by identifying, prioritizing and tracking the progress of remediation actions for all identified cybersecurity weaknesses; and

4. Include complete information for both Federal- and contractor-managed cybersecurity programs when reporting the status of performance metrics annually to DHS.

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 identified issues. For instance, management stated that the specific weaknesses identified in our report would be included in the Department's plan of action and milestones. In addition, management stated that it would enhance its capabilities to assess the plans of action and milestones for completeness and accuracy and initiate processes to validate information. Management also commented that it would continue to work to identify an effective means to capture cybersecurity metric data and ensure that a strategy is implemented to collect more accurate data in the various FISMA metric areas, particularly those related to the Administration's priorities.

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's (Department) unclassified cybersecurity program adequately protected its data and information systems.

Scope

We conducted the evaluation from February to October 2014, at 24 Department locations under the responsibility of the Under Secretary for 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 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 evaluation did not include a determination of whether the vulnerabilities were actually exploited. This audit was conducted under the Office of Inspector General Project Number A14TG026.

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 KPMG, LLP, the Office of Inspector General's contract auditor. Office of Inspector

General and KPMG, LLP 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.

- 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 objectives. 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.

An exit conference was held with management on October 22, 2014.

RELATED REPORTS

Office of Inspector General

- 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 of Energy's (Department) 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 Fiscal Year 2013, the Office of Inspector General identified eight areas, including cybersecurity, which remained a management challenge for the Department in Fiscal Year 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, the Naval Reactors Program had not always effectively utilized 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 the Laboratory's own policy related to ensuring that scanning was conducted to identify and mitigate security vulnerabilities in a timely manner.

- Audit Report on *Follow-up Audit of the Department's Cyber Security Incident Management Program* (DOE/IG-0878, December 2012). 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 cybersecurity 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 cybersecurity incident management strategy. In addition, changes to the Department's Incident Management Program 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 cybersecurity incident management program, a decentralized and fragmented approach had evolved that placed 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 Department had taken steps over the past year to address previously identified cybersecurity weaknesses and enhance its unclassified cybersecurity 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 cybersecurity 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 Western Area Power Administration had made a number of enhancements to its cybersecurity program since our prior review. However, several weaknesses related to vulnerability management and security controls existed that could negatively impact its cybersecurity posture. Specifically, Western Area Power Administration had not always implemented cybersecurity 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.

Government Accountability Office

- Report on *INFORMATION SECURITY: Federal Agencies Need to Enhance Responses to Data Breaches* (GAO-14-487T, April 2014).

- Report on *INFORMATION SECURITY: Agencies Need to Improve Cyber Incident Response Practices* (GAO-14-354, April 2014).

- Report on *FEDERAL INFORMATION SECURITY: Mixed Progress in Implementing Program Components; Improved Metrics Needed to Measure Effectiveness* (GAO-13-776, September 2013).

- Report on *CYBERSECURITY: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges* (GAO-13-462T, March 2013).

- Report on *HIGH-RISK SERIES: An Update* (GAO-13-283 and GAO-13-359T, February 2013).

- Report on *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 14, 2014

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

FROM: DONALD E. ADCOCK
CHIEF INFORMATION OFFICER, ACTING

SUBJECT: Inspector General's Draft Evaluation Report on "The Department's Unclassified Cyber Security Program – 2014"

Thank you for the opportunity to comment on the Draft Evaluation Report, "The Department's Unclassified Cyber Security Program - 2014." 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.

As we approach the FY 2015 audit, we would like to continue to work with the Office of the Inspector General and KPMG to improve and ensure the audit approach for evaluating systems considers the defense-in-depth strategies deployed for the protection of system(s).

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 Department of Energy (DOE) Program in a Plan of Action and Milestone (POA&Ms) report. Each DOE Program provides the estimated weakness completion dates and corrective actions 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. It is anticipated that the Programs will begin reporting on these findings in their first quarter fiscal year (FY) 2015 report.

In addition, the Office of the Chief Information Officer (OCIO) will enhance its capabilities to assess Program POA&M reports for completeness and accuracy and initiate processes to validate POA&M information. OCIO will include applicable findings is its program-level POA&M report for first quarter FY 2015.

Estimated Completion Date: 1st quarter FY 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, *Department of Energy Cyber Security Program*, codifies a federated risk-based approach to cybersecurity planning across the Department and establishes line management accountability. The Order has been updated three times since December 2012, adding requirements for the complete documentation of security requirements in information technology acquisitions and for the development and documentation of Program supply chain risk management processes. The Program Risk Management Implementation Plans (RMIPs) required by the Order will be updated to include these requirements as well as the requirements of the original issuance of this Order in 2011. These RMIPs include the development and implementation of procedures, processes, and performance measures to secure information, information systems and applications and assess the effectiveness of those procedures and processes.

Procedure and process weaknesses noted in this report have been reviewed by the Program Offices and corrective actions will be developed and managed as program-level POA&Ms.

Estimated Completion Date: 4th quarter FY 2015

Recommendation 3. *Fully develop and use plans of actions and milestones to improve its performance monitoring program by identifying, prioritizing and tracking the progress of remediation actions for all identified cybersecurity weaknesses.*

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. As noted in the response to Recommendation 1, the OCIO is enhancing its validation and assessment capabilities for POA&Ms and is leveraging its Enterprise Cyber Governance System (ECGS) to streamline POA&M tracking and reporting and provide a centralized repository for cybersecurity weakness remediation activities. This combined approach will assist the Program Offices in refining their processes for managing remediation activities, assessing weaknesses across the Program, and prioritizing actions. 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.

Estimated Completion Date: 4th quarter FY 2015

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.

The capture of FISMA metrics information on all Departmental activities 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 metrics data and will ensure that a strategy is implemented to garner more accurate data in the areas of FISMA metrics, and particularly relative to the Cross-Agency Priority goals. The FY14 annual FISMA report will be completed and submitted by the OMB-required due date.

Estimated Completion Date: 4th quarter FY 2015

If you have any questions or need additional information, please contact Mr. Rodney Turk, 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 OIGReports@hq.doe.gov and include your name, contact information and the report number. Comments may also be mailed to:

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.