OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

EVALUATION REPORT

DOE-OIG-17-01

October 2016

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2016

Department of Energy
Washington, DC 20585

October 14, 2016

MEMORANDUM FOR THE SECRETARY

FROM: Rickey R. Hass
Acting Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department of Energy's Unclassified Cybersecurity Program – 2016"

BACKGROUND

The use of information technology by Federal agencies continues to evolve, resulting in greater opportunities for accessibility to Government information and resources. With advancements in technology, however, cybersecurity incidents have become a prominent threat and are occurring at an increasing frequency. The Office of Management and Budget noted in its fiscal year (FY) 2015 report to Congress that Federal agencies reported an increase in volume and sophistication of cyber incidents. In addition, the Department of Energy continues to encounter various types of cybersecurity incidents including compromise of user workstations, Web defacements, and loss or theft of information technology equipment. In fact, the Department has reported more than 640 incidents in FY 2016.

The *Federal Information Security Modernization Act of 2014* requires 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. As required by the *Federal Information Security Modernization Act of 2014*, the Office of Inspector General conducted an 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 of the Department for FY 2016.

RESULTS OF EVALUATION

The Department, including the National Nuclear Security Administration, had taken a number of actions over the past year to address previously identified weaknesses related to its cybersecurity program. In particular, the Department made progress remediating weaknesses identified in our FY 2015 evaluation, which resulted in the closure of 10 of 12 prior year deficiencies. The Department also improved the completeness of its reporting of contractor system security information to the Department of Homeland Security and the Office of Management and Budget, an issue we had reported on for several years.

While these actions were positive, our current evaluation found that the types of deficiencies identified in prior years, including issues related to vulnerability management, system integrity of Web applications, access controls and segregation of duties, and configuration management, continue to exist. In particular, we found the following:

- Although improvements had been made, weaknesses continue to exist related to the Department’s vulnerability management program. Specifically, we identified that locations continued to use software on workstations and servers that was missing security patches or was no longer supported by the vendor. For instance, we determined that all workstations tested at two locations were missing current security patches for known vulnerabilities, even though the patches had been released more than 30 days prior to our testing.

- Deficiencies existed related to system integrity of Web applications. For example, our testing identified that applications used to support human resource, financial, and business activities accepted malicious input that could have been used to launch attacks against application users. Similar to prior years, we also noted that several applications stored user authentication information in an unsecure manner.

- Access control and/or segregation of duties weaknesses were identified at eight locations. For instance, we determined that three locations had not performed a periodic review of user access to ensure that privileges were required for the applications reviewed. In addition, three locations had weaknesses related to password management, including the use of blank or inappropriately shared passwords.

- Weaknesses existed at four locations related to configuration management programs. Specifically, our review of sampled configuration changes found that change requests were not always properly documented for two general support systems.

The weaknesses identified occurred, in part, because the Department had not fully developed and/or implemented policies and procedures related to the weaknesses identified in our report. For instance, we found that the implementation of configuration and security patch management processes had not ensured that software remained secure. In addition, Department officials had not always implemented an effective performance monitoring and risk management program, including the use of an effective cybersecurity continuous monitoring program. We continued to identify concerns with the Department’s management of plans of action and milestones to track corrective actions for its cybersecurity program.

In addition, although not contributing directly to each of the weaknesses identified in our report, we noted challenges throughout the Department related to ensuring that cybersecurity policies and procedures are updated in a timely manner to meet Federal requirements. Most notably, we found that the Department’s primary cybersecurity directive had not incorporated critical Federal requirements issued more than 3 years ago. In addition, as noted in several previous evaluations, the Office of Science had not updated its Program Cyber Security Plan since June 2010 to reflect new cybersecurity risks and changes to Federal or Department policy.

Without improvements to its cybersecurity program, such as enhanced controls over vulnerability management and system access, the Department's systems and information will continue to be at a higher-than-necessary risk of compromise, loss, and/or modification. In addition, absent a fully effective performance monitoring and risk management program, the Department may not adequately address cybersecurity risks to ensure protection of data and information systems. Furthermore, without improvements to ensure that the most current security requirements are implemented, programs and sites may not keep pace with the challenges facing an ever-changing cybersecurity landscape. Therefore, 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, we have omitted specific information and site locations from this report. We have provided site and program officials with detailed information regarding vulnerabilities that we identified at their locations, and in many cases, officials have 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 for the National Nuclear Security Administration
Deputy Under Secretary for Management and Performance
Chief of Staff
Chief Information Officer
Chief Financial Officer

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2016

TABLE OF CONTENTS

Evaluation Report

Appendices

DETAILS OF FINDING

The *Federal Information Security Modernization Act of 2014* (FISMA) requires the Office of Inspector General (OIG) to conduct an independent evaluation of the Department of Energy’s information security program and practices to determine whether the unclassified cybersecurity program adequately protects information systems and data. To support our FISMA evaluation, we conducted extensive control testing and assessments of the unclassified cybersecurity programs at 23 Department locations primarily under the purview of the Administrator for the National Nuclear Security Administration, Under Secretary for Science and Energy, and Under Secretary for Management and Performance. Our review included testing of networks and applications, scanning for technical vulnerabilities, and validating corrective actions taken to remediate prior year weaknesses. We also relied on results from ongoing and prior OIG audits and conducted testwork at six Department locations to support an evaluation against FISMA metrics issued by the Department of Homeland Security and the Office of Management and Budget. Furthermore, we considered the results of reviews conducted by the Department’s Office of Enterprise Assessments when reporting on the Department’s cybersecurity program.

Our fiscal year (FY) 2016 evaluation identified that the Department had taken significant action to address the deficiencies noted during our prior year evaluation, such as the following:

- Department programs had taken corrective actions related to vulnerability management, access controls, and maintaining the integrity of Web applications, which resulted in the closure of 10 of the 12 deficiencies reported during our prior year evaluation.

- The Department made significant improvements to report on the status of its entire cybersecurity program, to include information related to contractor systems. Specifically, we noted that contractor information was reported for 48 of 65 metrics in the Department’s FISMA submission to the Department of Homeland Security and the Office of Management and Budget. This represented more than a three-fold increase from the prior year.

Although the actions taken by the Department should help improve its cybersecurity posture, additional effort is needed to further enhance security over systems and information. Our review of 23 locations revealed that the identified vulnerabilities were similar in type to those identified during prior evaluations.

Unclassified Cybersecurity Program

Our FY 2016 evaluation identified weaknesses related to vulnerability management, system integrity of Web applications, access controls and segregation of duties, and configuration management. Although the types of vulnerabilities identified were consistent with our prior evaluation, our FY 2016 review disclosed weaknesses at a number of new locations and noted unresolved weaknesses from the prior year at two locations.

Vulnerability Management

The Department had taken action to address two of the vulnerability management deficiencies identified in our FY 2015 review related to information system assets that were operating without current security patches for known vulnerabilities or using default passwords. However, our testwork indicated that vulnerability management weaknesses existed at six locations, with problems of varying criticality. Specifically, our review determined the following:

- All workstations tested at two locations were operating without current security patches for known vulnerabilities, even though the patches had been released more than 30 days prior to our testing. For example, all workstations tested at one location were missing high or critical security updates and patches, resulting in various types of vulnerabilities. Furthermore, our ongoing audit of cybersecurity at an Office of Science (Science) location identified 243 unique vulnerabilities on information system assets, including 224 (92 percent) high or medium risk vulnerabilities.

- Four locations were running applications that the vendor no longer supported. For example, at one site we identified at least five unsupported software applications. In addition, one site was running unsupported client applications on more than half of the workstations tested.

- One site reported 571 unique vulnerabilities (75 critical and 496 high) during our testwork, some of which were discovered more than 10 years ago. Officials explained that many of these vulnerabilities existed on numerous types of devices and legacy systems. To their credit, subsequent to our testwork, site officials stated they took action to significantly reduce the number of high and critical vulnerabilities.

- Although one location addressed deficiencies noted in our prior review, it had not fully implemented the vulnerability management program as recommended. Specifically, the site did not review and verify the accuracy of system information, update its asset inventory, or ensure that information assets were receiving virus signature updates in a timely manner. Without an effective virus protection program, information assets are at risk for computer viruses and other malicious attacks that may affect data integrity and confidentiality.

We found that locations implemented certain controls to mitigate risks associated with security weaknesses. However, we determined that the mitigating controls may not always be sufficient to provide reasonable assurance that patches would be applied and vulnerabilities were remediated in a timely manner. The failure of such controls could result in unauthorized access to systems and information, as well as loss or disruption to critical operations. In addition to our testing, the Department's Office of Enterprise Assessments reported on vulnerability management weaknesses at numerous sites throughout FY 2016.

System Integrity of Web Applications

We identified numerous weaknesses related to system integrity of Web applications at six locations. Our testwork found that Web applications used to support human resource, financial, and business functions did not properly validate input data and/or protect the confidentiality of user credentials. This increased the risk of malicious attacks that could result in unauthorized access to the applications and sensitive data. Our review found the following:

- Eight applications tested at five locations accepted malicious input data that could be used to launch attacks against legitimate application users. These types of 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. In addition, one of the eight applications did not validate input data and allowed the data to be used in a way that made the application vulnerable to attacks against the application's database server. This type of attack could result in unauthorized access to application functionality and the modification of information stored within the database.

- At four locations, we identified six applications that stored user authentication information in an unsecure manner on the network, making the authentication information accessible to any Web server on the same network. Web applications that do not properly protect the confidentiality of user authentication information are at an increased risk of unauthorized access to the application and sensitive data stored within the system.

- One application did not properly enforce access controls, a situation that could have allowed users with lower privileges to browse to Web pages that should have been restricted to higher privileged users. Once at the restricted page, lower privileged users could have accessed data and performed functions that were reserved for users with higher privileges.

- One location had made progress addressing prior year weaknesses related to managing Web applications. However, it had not completed corrective actions to identify and remediate Web application vulnerabilities and ensure that input data was validated before the application accepted it for further processing. A successful attack against this weakness could have compromised segregation of duties rules and resulted in unauthorized changes to data and disclosure of sensitive information.

During FY 2016, the Office of Enterprise Assessments noted similar issues at four locations. Web application weaknesses, such as those noted above, could also have negative impacts on the security of information systems, as well as application and data reliability.

Access Controls and Segregation of Duties

Notably, the Department had taken steps to correct access control related weaknesses identified during our prior year review. However, our current evaluation identified several new deficiencies related to access controls and segregation of duties. Specifically, we noted weaknesses in the following areas:

- One location had not uniquely identified and authenticated database administrators of two databases. Specifically, database administrators inappropriately used default administrative accounts for identification. In addition, account authorization forms were not maintained to identify users and assign and authorize privileges. The deficiencies noted could result in individual accountability weaknesses for database administrator activities, such as creating and granting roles when using shared accounts.

- Three locations had not performed a periodic review of user access for the applications reviewed. For instance, one location had not periodically reviewed shared database administrative accounts. Failing to perform periodic user access reviews may increase the risk of inappropriate access to applications. In addition, we noted that officials at one location had not removed terminated users' access from an application within required timeframes.

- Password management weaknesses existed at three locations reviewed. At one location, system administrators used a blank password for an administrator account used to manage firewalls, switches, and other networking devices. We found that the other location routinely shared passwords among database administrators, which is contrary to Federal and site-level requirements.

- As part of our testing against the FISMA metrics, we found that the vast majority of sites reviewed had not used personal identity verification card credentials to permit system access for all privileged users and 85 percent of non-privileged users. While the Department had developed an implementation approach, it recently reported in its monthly performance submission to the Office of Management and Budget that only 57 percent of privileged users and 21 percent of non-privileged users were using personal identity verification cards to authenticate to information systems. This issue was recently highlighted as an area of focus by the Office of Management and Budget and is the subject of an OIG review that was in progress at the time this report was issued.

- Segregation of duties weaknesses existed at one location. We determined that individuals were assigned conflicting roles within a financial application and that the conflicting roles had existed for an extended period, as far back as 2004. Unnecessary privileges assigned to users to perform assigned tasks may increase the risk of unauthorized configuration changes and user profile modifications. In addition, the risk of unintentional errors and possible malicious behavior may increase and could result in data modification.

Access control weaknesses were also identified in our report on *The Energy Information Administration's Technology Program* (DOE-OIG-16-04, November 2015). Specifically, we found that application functionality allowed for the potential bypass of access controls due to the use of default credentials and lack of input data validation. Similar to the issues we identified during our reviews, the Office of Enterprise Assessments also reported on a number of access control deficiencies at five locations reviewed during FY 2016.

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 systemically controls changes to that configuration during the system's life cycle. At two locations reviewed, we found that information system change requests were not always properly documented. For example, changes were implemented without management approval and tested/implemented without test plans and documented test results. Due to the confirmed lack of documentation, we were unable to determine whether changes were successfully tested prior to implementation in the production environment. Although we identified compensating controls to mitigate risk at both locations, we determined that the weaknesses identified could have an impact on security over the general support systems.

Cybersecurity Program Management

The weaknesses identified occurred, in part, because the Department had not fully developed and/or implemented policies and procedures related to the weaknesses noted in our report. In addition, as indicated in our prior report, the Department had not always implemented an effective performance monitoring and risk management program, including the use of an effective cybersecurity continuous monitoring program.

Policies and Procedures

Programs and sites had not always developed policies and procedures to ensure fully effective security controls over systems and information. In particular, we found that a number of locations had not established complete procedures related to areas such as vulnerability management, access controls, and system integrity of Web applications. In at least one instance, we noted that security patch management processes were not adequate to ensure that unsupported software was upgraded to a supported version or removed in a timely manner. In addition, we determined that two locations' vulnerability management programs had not included adequate Web application testing procedures to identify vulnerabilities related to data confidentiality and integrity of authentication functionality and access control configurations in Web applications.

Even when policies and procedures were documented, they were not always fully implemented. For example, we found that robust patch management procedures had not been implemented to effectively remediate vulnerabilities affecting information system assets. We noted that three sites had not fully implemented security patch management processes over information systems. Contrary to existing procedures, the sites had not ensured that security updates and patches for known vulnerabilities and/or outdated software were applied in a timely manner. We found that, in one case, site officials had not coordinated vulnerability scanning processes with energy savings goals, resulting in workstations that were shut down during times of after-hours scanning. Officials commented that, subsequent to our review, they had replaced all evaluated machines and improved the patching process.

Similarly, we determined that officials had not always implemented existing policies and procedures related to access controls and configuration management. Specifically, officials at several locations had not followed their access control procedures related to ensuring annual reviews of user access or enforced minimum password requirements throughout the computing environment. In addition, even though a configuration management plan for infrastructure change requests existed, one site had not followed the plan and fully implemented effective separation of duties related to configuration changes over the system reviewed.

Performance Monitoring and Risk Management

The Department had not implemented a fully effective performance monitoring and risk management program. Consistent with prior year FISMA evaluations, we noted problems with the Department's plan of action and milestones (POA&M) process. This process is an important tool required to assist management in identifying, prioritizing, and tracking remediation activities for known cybersecurity vulnerabilities. While we found that the vast majority of weaknesses identified during our FY 2015 evaluation were included in POA&Ms submitted to the Office of the Chief Information Officer, we continued to identify concerns:

- The percentage of open milestones that were past the scheduled completion date substantially increased since our prior year evaluation. In particular, our analysis found that 851 of 1,093 open milestones (78 percent) were overdue. Of those, 53 percent were at least 1 year beyond the estimated completion date.

- POA&Ms were not effectively utilized to track, prioritize, and remediate weaknesses at three locations reviewed. Specifically, we found that one location was internally tracking POA&M items, but items were not reported to the Office of the Chief Information Officer. Another location was unable to provide documentation to support that the POA&Ms were reviewed by the cognizant program office. Furthermore, an ongoing OIG review found that one site had not included all self-identified weaknesses in its POA&M process. The Office of Enterprise Assessments reported similar issues at six locations reviewed during FY 2016.

We also determined that continuous monitoring and risk management processes at several locations reviewed were not always effective to identify and remediate cybersecurity weaknesses. Specifically, many of the vulnerabilities we identified occurred because officials had not ensured that adequate safeguards were in place and operating effectively to identify and remediate Web application vulnerabilities. For example, application security or vulnerability management programs at three locations did not include adequate Web application testing procedures. At another location, the vulnerability management process did not include validation procedures to ensure complete coverage of application functionality during scans. Officials at another site did not always perform detailed vulnerability scanning, including scans using authenticated credentials, to identify missing security patches.

Risk to Information and Systems

Without improvements to address the weaknesses identified in our report, the Department's information and systems will continue to be at a higher-than-necessary risk of compromise, loss, and/or modification. The OIG has continuously recognized cybersecurity as a management challenge area for the Department, emphasizing the critical need to enhance the Department's overall security posture. We found that deficiencies in developing, updating, and/or implementing policies and procedures may adversely affect the Department's ability to properly secure its information technology assets. Furthermore, without a fully effective process for tracking corrective actions using POA&Ms, the Department may not have a complete understanding of the status of the cybersecurity program and the current risks to the program. Although sites had implemented compensating controls to mitigate a number of the weaknesses identified during our review, our testwork found that an attacker could exploit the existing vulnerabilities. Therefore, additional action is necessary to help strengthen the Department's unclassified cybersecurity program.

Cybersecurity Framework Challenges

Although not contributing directly to each of the weaknesses identified in our report, we have noted challenges throughout the Department related to ensuring that cybersecurity policies and procedures are updated in a timely manner to meet Federal requirements. Most notably, we found that the Department's primary cybersecurity directive, Department Order 205.1B, *Department of Energy Cyber Security Program*, continues to reference outdated guidance from the National Institute of Standards and Technology rather than reference its Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, which was published in April 2013. This issue was highlighted in our recent report on *The Energy Information Administration's Information Technology Program*, which noted that 10 controls and 37 control enhancements included in the new guidance may not have been implemented related to areas such as access controls and configuration management. Similar issues were identified in our ongoing review of the cybersecurity program at a Science location. In addition, as noted in several previous evaluations, Science had not updated its Program Cyber Security Plan since June 2010 to reflect new cybersecurity risks and changes to Federal or Department policy. While we have a long-standing recommendation in this area, Science officials have yet to take corrective actions, potentially affecting the security posture of its program and sites. Without improvements to ensure that the most current security requirements are implemented, programs and sites may not keep pace with the challenges facing an ever-changing cybersecurity landscape.

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 during our review and highlighted in this report; and

2. Fully develop and utilize POA&Ms to improve performance monitoring by identifying, prioritizing, and tracking the progress of remediation actions for all identified cybersecurity weaknesses.

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:

3. Update and implement Department and program-level cybersecurity policies and procedures in a timely manner to ensure consistency with Federal requirements.

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 example, management stated that the weaknesses noted in the report have been reviewed and the appropriate Department program will identify corrective actions. In addition, management stated it would continue work for full implementation of the enterprise POA&M tracking tool. Also, management commented that the Department's revision to Order 205.1B is currently scheduled to be complete by June 2017. Further, management indicated that the Office of Science Program Cyber Security Plan is undergoing final review, with an expected final version to be released in the first quarter of FY 2017.

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 unclassified cybersecurity program adequately protected its data and information systems.

Scope

We conducted the evaluation from February 2016 to October 2016 at 23 Department locations primarily under the responsibility of the Administrator for the National Nuclear Security Administration, Under Secretary for Science and Energy, Under Secretary for Management and Performance, and the Administrator of the 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 (OIG) related to the Department's cybersecurity program. This evaluation was conducted under OIG project number A16TG025.

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, 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 OIG's contract auditor, KPMG LLP (KPMG). OIG 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.

- Conducted reviews to respond to *Federal Information Security Modernization Act of 2014* metrics established by the Department of Homeland Security and the Office of Management and Budget. The reviews were conducted at six locations across various Department programs/elements.

- Evaluated and incorporated the results of other cybersecurity reviews performed by the OIG, the Government Accountability Office, and the Office of Enterprise Assessments' Office of Cyber Assessments.

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 the *Federal Information Security Modernization Act of 2014*, 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 on October 12, 2016.

RELATED REPORTS

Office of Inspector General

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program - 2015* (DOE-OIG-16-01, November 2015). The Department of Energy, 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 fiscal year (FY) 2014 evaluation, which resulted in the closure of 22 of 26 reported deficiencies. While these actions were positive, our 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. 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. Furthermore, we noted that risk management processes at locations reviewed were not always effective to identify and remediate cybersecurity weaknesses.

- Special Report on *Management Challenges at the Department of Energy – Fiscal Year 2016* (OIG-SR-16-01, November 2015). Based on the work performed during FY 2015, the Office of Inspector General (OIG) identified seven areas, including cybersecurity, that remained management challenges for FY 2016.

- Audit Report on *The Energy Information Administration's Information Technology Program* (DOE-OIG-16-04, November 2015). Our review largely substantiated the allegations related to information technology (IT) and records management. Based on these findings, we determined that the Energy Information Administration (EIA) had not implemented a fully effective IT program. In particular, we identified weaknesses related to IT project management, capital planning and investment control, cybersecurity, and records management. The weaknesses identified occurred, in part, because EIA management had not ensured that applicable Federal and Department policies and procedures were always implemented. Furthermore, EIA had not implemented an effective governance structure over IT project management and cybersecurity activities. Confusion regarding lines of authority adversely affected EIA's cybersecurity, project management, and records management programs. We noted that a number of weaknesses related to these areas may have been alleviated had EIA implemented a centralized approach to management.

- Audit Report on *The Department of Energy's Cybersecurity Risk Management Framework* (DOE-OIG-16-02, November 2015). Our review found that although progress had been made toward implementing an unclassified cybersecurity risk management framework designed to reduce the likelihood of compromise to its information systems and data, additional effort was needed to ensure that operating system risks are identified and systems and information are adequately secured. Although certain controls had been established, officials had not always thoroughly and independently assessed or monitored such controls to ensure that they were effective. Furthermore, programs and sites had not ensured that Authorizing Officials responsible for accepting system risk were fully aware of the risks, weaknesses, and vulnerabilities to the information systems under their purview. The weaknesses identified existed, in part, because Federal requirements for securing information systems had not been fully implemented, and the Department had not established sufficient oversight and communication to support its cybersecurity risk management program. In addition, Federal officials had not provided adequate oversight to ensure that effective risk management practices had been implemented and Department management had not always ensured that risk tolerances were established and communicated to field elements as required to help ensure the implementation of an effective risk management program.

- 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 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 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 OIG identified six areas, including cybersecurity, that remained management challenges 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 contractors. We concluded that the July 2013 incident resulted in the exfiltration of personally identifiable information on more than 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 OIG identified eight areas, including cybersecurity, that remained management challenges 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.

Government Accountability Office

- *INFORMATION SECURITY: Agencies Need to Improve Controls over Selected High-Impact Systems* (GAO-16-501, May 2016)

- *INFORMATION SECURITY: Department of Education and Other Federal Agencies Need to Better Implement Controls* (GAO-16-228T, November 2015)

- *INFORMATION SECURITY: Federal Agencies Need to Better Protect Sensitive Data* (GAO-16-194T, November 2015)

- *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)

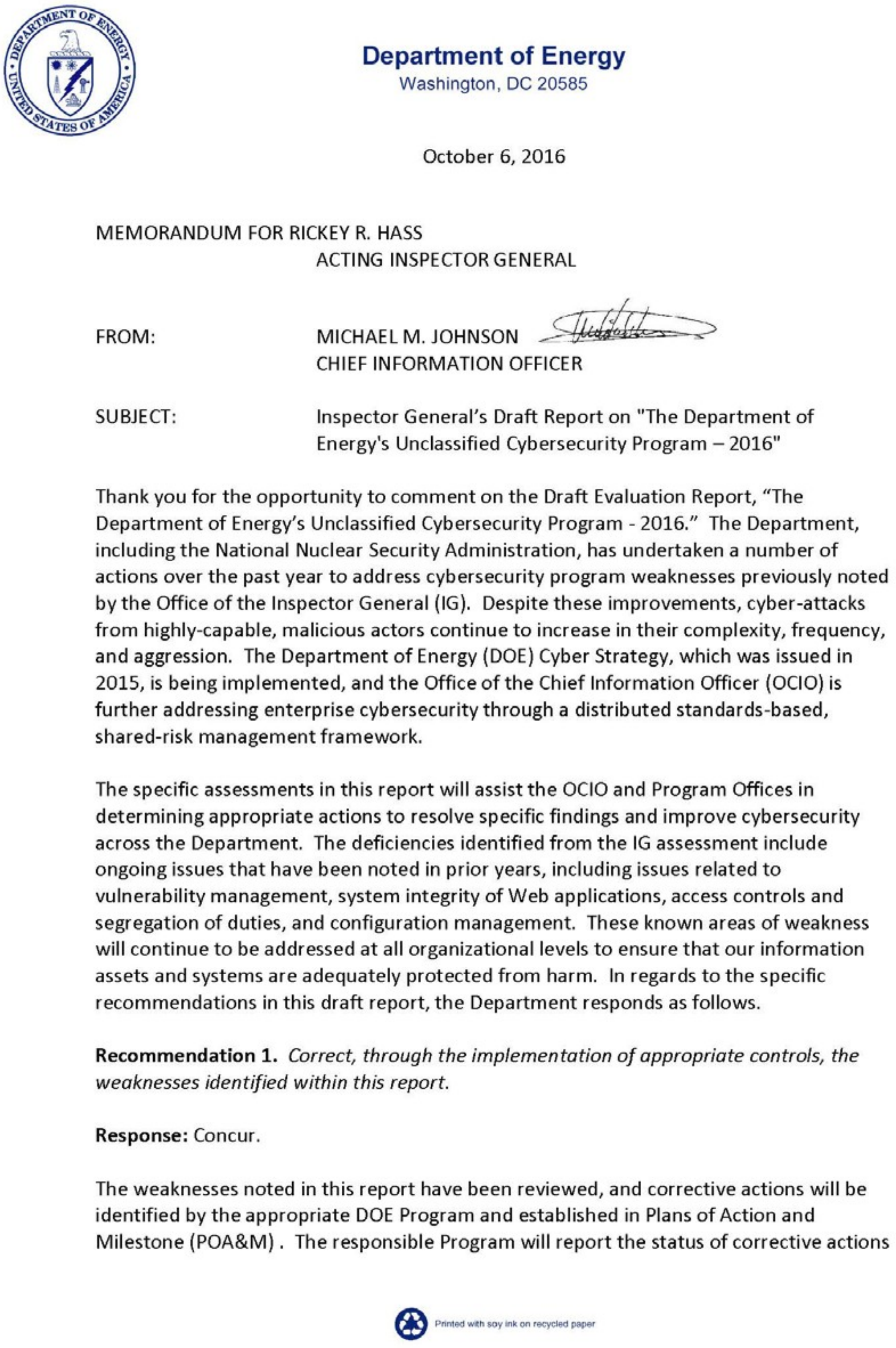
- *CYBERSECURITY: Recent Data Breaches Illustrate Need for Strong Controls across Federal Agencies* (GAO-15-725T, June 2015)

- *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)

APPENDIX 3

MANAGEMENT COMMENTS



Department of Energy
Washington, DC 20585

October 6, 2016

MEMORANDUM FOR RICKEY R. HASS
ACTING INSPECTOR GENERAL

FROM: MICHAEL M. JOHNSON
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General's Draft Report on "The Department of Energy's Unclassified Cybersecurity Program – 2016"

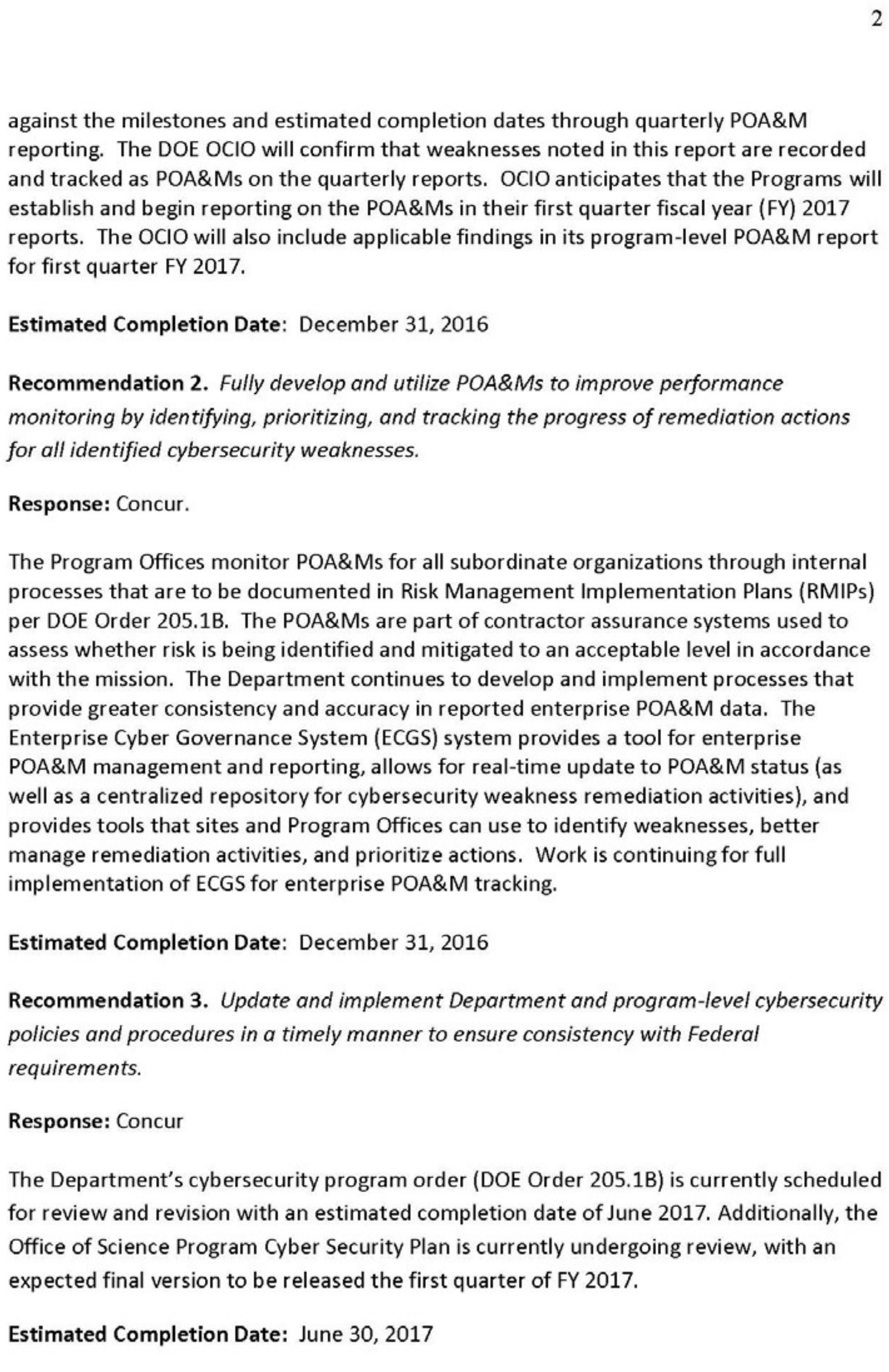
Thank you for the opportunity to comment on the Draft Evaluation Report, "The Department of Energy's Unclassified Cybersecurity Program - 2016." The Department, including the National Nuclear Security Administration, has undertaken a number of actions over the past year to address cybersecurity program weaknesses previously noted by the Office of the Inspector General (IG). Despite these improvements, cyber-attacks from highly-capable, malicious actors continue to increase in their complexity, frequency, and aggression. The Department of Energy (DOE) Cyber Strategy, which was issued in 2015, is being implemented, and the Office of the Chief Information Officer (OCIO) is further addressing enterprise cybersecurity through a distributed standards-based, shared-risk management framework.

The specific assessments in this report will assist the OCIO and Program Offices in determining appropriate actions to resolve specific findings and improve cybersecurity across the Department. The deficiencies identified from the IG assessment include ongoing issues that have been noted in prior years, including issues related to vulnerability management, system integrity of Web applications, access controls and segregation of duties, and configuration management. These known areas of weakness will continue to be addressed at all organizational levels to ensure that our information assets and systems are adequately protected from harm. 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 and established in Plans of Action and Milestone (POA&M) . The responsible Program will report the status of corrective actions



against the milestones and estimated completion dates through quarterly POA&M reporting. The DOE OCIO will confirm that weaknesses noted in this report are recorded and tracked as POA&Ms on the quarterly reports. OCIO anticipates that the Programs will establish and begin reporting on the POA&Ms in their first quarter fiscal year (FY) 2017 reports. The OCIO will also include applicable findings in its program-level POA&M report for first quarter FY 2017.

Estimated Completion Date: December 31, 2016

Recommendation 2. *Fully develop and utilize POA&Ms to improve performance monitoring 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 Risk Management Implementation Plans (RMIPs) per DOE Order 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 Department continues to develop and implement processes that provide greater consistency and accuracy in reported enterprise POA&M data. The Enterprise Cyber Governance System (ECGS) system provides a tool for enterprise POA&M management and reporting, allows for real-time update to POA&M status (as well as a centralized repository for cybersecurity weakness remediation activities), and provides tools that sites and Program Offices can use to identify weaknesses, better manage remediation activities, and prioritize actions. Work is continuing for full implementation of ECGS for enterprise POA&M tracking.

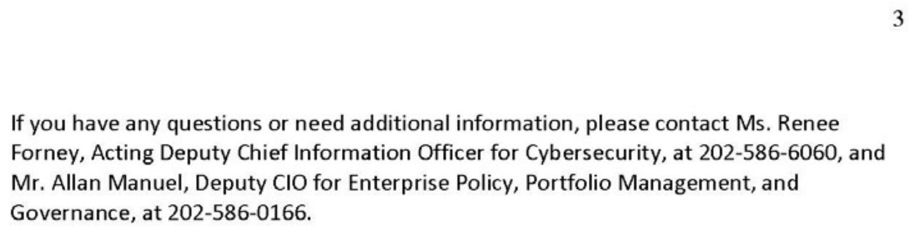
Estimated Completion Date: December 31, 2016

Recommendation 3. *Update and implement Department and program-level cybersecurity policies and procedures in a timely manner to ensure consistency with Federal requirements.*

Response: Concur

The Department's cybersecurity program order (DOE Order 205.1B) is currently scheduled for review and revision with an estimated completion date of June 2017. Additionally, the Office of Science Program Cyber Security Plan is currently undergoing review, with an expected final version to be released the first quarter of FY 2017.

Estimated Completion Date: June 30, 2017



If you have any questions or need additional information, please contact Ms. Renee Forney, Acting Deputy Chief Information Officer for Cybersecurity, at 202-586-6060, and Mr. Allan Manuel, Deputy CIO for Enterprise Policy, Portfolio Management, and Governance, 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.