OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

EVALUATION REPORT

DOE-OIG-19-01

October 2018

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2018

Department of Energy
Washington, DC 20585

October 19, 2018

MEMORANDUM FOR THE SECRETARY

FROM: April G. Stephenson
Acting Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department of Energy's Unclassified Cybersecurity Program – 2018"

BACKGROUND

The use of information technology by Federal agencies continues to evolve, resulting in greater opportunities for efficiencies and accessibility to Government information. The Department of Energy operates many facilities, including National Laboratories and plants, across the Nation and depends on information technology systems and networks for essential operations required to accomplish its national security, research and development, and environmental management missions. Advancements in technology, however, can result in increased cybersecurity threats. For instance, the systems used to support the Department's various missions face millions of cyber threats each year, ranging from unsophisticated hackers to advanced persistent threats using state-of-the-art intrusion tools and techniques. Many of these malicious attacks are designed to steal information and disrupt, deny access, degrade, or destroy the Department's information systems.

The *Federal Information Security Modernization Act of 2014* requires Federal agencies to develop and implement 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 fiscal year 2018.

RESULTS OF EVALUATION

We determined that opportunities existed for the Department, including the National Nuclear Security Administration, to enhance its ability to protect information systems and data. The Department had taken actions over the past year to address previously identified weaknesses related to its cybersecurity program. In particular, programs and sites made progress remediating weaknesses identified in our fiscal year 2017 evaluation, which resulted in the closure of all 12

prior year weaknesses. Although these actions were positive, our current evaluation identified weaknesses that were mostly consistent with our prior reports related to vulnerability and configuration management, system integrity of Web applications, access controls, security awareness and privacy training, and security control testing. In particular, we found the following:

- Although improvements were made, weaknesses continue to exist related to the Department's vulnerability and configuration management programs. Specifically, at least 10 locations continued to use software on workstations and servers that were missing security patches or were no longer supported by the vendor. We also noted that one of these sites had not conducted privileged vulnerability scans on all devices – a key component of a fully effective vulnerability management program that can help identify weaknesses. Furthermore, another site excluded a significant number of vulnerabilities identified during our testing from its remediation efforts. While we identified weaknesses at each of the 10 locations, a number of them had either documented the acceptance of risk or had developed corrective action plans with respect to the vulnerabilities identified.

- Weaknesses related to system integrity of Web applications were identified at two locations, including improper validation of input data and/or the protection of the confidentiality of user credentials. Weaknesses such as these could have allowed an attacker to gain unauthorized access to an application, make unauthorized changes to data, and disclose sensitive information.

- Access control weaknesses were identified at four locations. Specifically, our test work uncovered weaknesses related to the disablement of user accounts, inadequate use of least privilege and/or segregation of duties, and a lack of adequate enforcement of access controls on Web applications.

- Weaknesses related to the Department's security awareness and privacy training were identified at three locations. In particular, sites reviewed had not developed and/or implemented role-based security training for all users. In addition, sites reviewed had a significant number of users with overdue training when compared to the required frequency described within site policy. One site also had not provided annual privacy awareness training in accordance with Department requirements.

- One site could not demonstrate that it had completed a thorough assessment of all required security controls as part of its continuous monitoring process. In particular, documentation provided to support its assessment of controls was incomplete and did not illustrate that many required controls were assessed in accordance with guidance set forth within National Institute of Standards and Technology Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*.

The weaknesses identified occurred, in part, because Department officials had not fully developed and/or implemented policies and procedures related to issues identified in our report.

For instance, we noted that certain sites lacked adequate policies and procedures related to cybersecurity training, and vulnerability and configuration management programs. Even when policies and procedures did exist, they were not always implemented by site officials. In addition, we determined that the sites reviewed had not always implemented an effective risk management program. For example, risk management methodologies at certain locations placed limitations on the effectiveness of their vulnerability management programs. Further, while not directly contributing to the specific weaknesses identified during our test work, we also found that many cybersecurity weaknesses continued to exist because plans of action and milestones had not been corrected in a timely manner.

Absent improvements to address the weaknesses identified in our report, the Department's information systems and data may be at a higher-than-necessary risk of compromise, loss, and/or modification. The Office of Inspector General has continuously recognized cybersecurity as a management challenge area for the Department, emphasizing the critical need to enhance the Department's overall security posture. In addition, the Office of Inspector General and other independent reviewers continue to identify vulnerabilities related to developing, updating, and/or implementing policies and procedures that may adversely affect the Department's ability to properly secure its information systems and data. Without the implementation of effective cybersecurity controls, the weaknesses noted during our review may increase the risk of unauthorized modification to information systems and the data they contain. Therefore, additional action is necessary to help strengthen the Department's unclassified cybersecurity program. We made numerous recommendations to the locations reviewed that are designed to improve their cybersecurity posture.

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 vulnerabilities.

MANAGEMENT RESPONSE

Management concurred with the report's recommendation and indicated that corrective actions 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.

Attachment

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

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2018

TABLE OF CONTENTS

Evaluation Report

Appendices

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2018

BACKGROUND

The *Federal Information Security Modernization Act of 2014* requires the Office of Inspector General to conduct an annual independent evaluation to determine whether the Department of Energy's unclassified cybersecurity program adequately protected its data and information systems. To support our evaluation, we conducted control testing and assessments of various aspects of the unclassified cybersecurity programs at 27 Department locations primarily under the purview of the National Nuclear Security Administration, Under Secretary for Science, Under Secretary of Energy, and other staff offices. 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 Office of Inspector General reviews, including test work conducted at five Department locations to support an evaluation against *Federal Information Security Modernization Act of 2014* security 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) 2018 evaluation determined that the Department had taken actions to address weaknesses noted during our prior year evaluation. Specifically, Department programs and sites had taken corrective actions related to vulnerability and configuration management, access controls, and integrity of Web applications, which resulted in the closure of all weaknesses reported during our prior year evaluation. 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 27 locations revealed that the identified vulnerabilities were similar in type to those identified during prior evaluations. Throughout our report, we generally refer to locations where findings and recommendations were issued even though similar weaknesses may have been identified at additional locations.

DETAILS OF FINDINGS

Our FY 2018 evaluation identified weaknesses related to vulnerability and configuration management, system integrity of Web applications, access controls, cybersecurity and privacy awareness training, and security control testing. Although the types of vulnerabilities identified were mostly consistent with our prior evaluations, our FY 2018 review disclosed weaknesses at new locations.

Vulnerability and Configuration Management

The Department had taken action to address and close all of the vulnerability and configuration management weaknesses identified in our prior reviews. However, our test work indicated that vulnerability and configuration management weaknesses continued to exist, resulting in seven new findings. Vulnerability management is the process in which weaknesses are identified and the risks of those weaknesses are evaluated. The evaluation of those risks leads to either the mitigation of the weakness or the formal acceptance of the risks. Our review determined the following:

- Although one site deployed an automated scanning tool for its information systems and periodically scanned systems and applications for potential vulnerabilities, weaknesses existed within the vulnerability management process. Specifically, we determined that the location had not conducted privileged, or authenticated, vulnerability scans against all servers and workstations to increase the effectiveness of the vulnerability management program. Although officials indicated that privileged scans were conducted on certain operating systems encompassing the majority of workstations, they had not conducted privileged scans for workstations running other types of operating systems. Without the use of privileged scanning, the identification and related remediation of security weaknesses may be limited. Officials indicated that they were in the process of transitioning to secure host-based scans in place of network-based privileged scans.

- Nine locations were running applications that were no longer supported by the vendor. When a product reaches its end-of-life and is no longer supported by the vendor, the vendor does not release new security patches for the product, increasing the risk of compromise. At one of the locations, our review identified an application server that the vendor had not supported since 2015, as well as an operating system that the vendor had not supported since July 2010. Officials indicated that the risk related to this weakness was accepted and mitigating controls were in place.

- Although one site conducted regularly scheduled vulnerability scans, many vulnerabilities were not considered for remediation. Specifically, we noted that the site based its approach and methodology for vulnerability remediation on those issues with a publicly available exploit, as reported by its vulnerability scanning tool. Our test work identified at least 934 critical and high-risk vulnerabilities that were excluded from the site's remediation process. To further exacerbate the issues surrounding the remediation of vulnerabilities at this location, we also determined that it had not fully implemented a process for evaluating and measuring progress of addressing medium-risk vulnerabilities.

- One site was using a specific management and monitoring network protocol that could allow passwords to be obtained and enable unauthorized remote access to the affected systems. Remediation of this type of vulnerability would have required the site to conduct additional research and actions, as remediation involves more than applying a missing patch/updates or upgrading installed software.

- At one location, we identified several vulnerabilities related to unsupported applications and client applications that were missing security updates on workstations and servers. However, officials indicated that these vulnerabilities existed due to the ongoing efforts of the site's project to upgrade its vulnerability management capabilities.

Overall, our test work revealed that sites across each of the three Under Secretary organizations reviewed had vulnerable servers and/or workstations missing security patches for known critical and high-risk vulnerabilities at least 30 days prior to our testing. Our limited scans found that nearly half of the workstations tested at 10 locations had either critical or high-risk vulnerabilities. For instance, we determined that 55 of 60 (92 percent) workstations tested at 1 location contained such vulnerabilities. Furthermore, nearly one-third of servers tested at nine locations had either

critical or high-risk vulnerabilities. For instance, we identified 1 site which had critical and/or high-risk vulnerabilities on 268 of 287 (94 percent) of servers tested. Although officials at this site indicated that these vulnerabilities were accepted as part of the site's risk management process, we remain concerned with the high number of weaknesses. At another location, we noted that officials had not appropriately documented and/or accepted the risk of operating vulnerable applications.

Our evaluation also identified a weakness related to the management of baseline configurations at one site. As part of a holistic risk management strategy and applying the information security concept of defense-in-depth, organizations are required to employ appropriate configuration settings for organizational systems. However, we determined that one site had not selected or documented an approved configuration baseline for a set of databases. The use of secure configurations that emphasize hardening of systems against flaws in software can result in greater levels of security and protection from future threats.

We concluded that locations implemented certain controls to mitigate risks associated with security weaknesses. However, we determined that the mitigating controls may not always be effective and 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 during FY 2018.

System Integrity of Web Applications

While the Department had taken action to remediate prior year findings, we identified weaknesses related to system integrity of Web applications at two locations. Specifically, our test work found that Web applications used to support key business functions did not properly validate input data and/or protect the confidentiality of user credentials. The identified Web applications at the locations reviewed did not always prevent malicious input data that could be used to launch attacks against legitimate application users. These types of attacks, known as cross-site scripting, could have allowed an attacker to gain unauthorized access to an application, make unauthorized changes to data, and disclose sensitive information. Maintaining effective system integrity controls over Web applications can decrease the risk of unauthorized access to and/or modification of sensitive information in the applications.

Access Controls and Segregation of Duties

The Department had taken steps to correct each of the access control related weaknesses identified during our prior year review. Access controls determine the allowed activities of legitimate users and mediate every attempt by a user to access a resource in the system. Our current evaluation identified several new weaknesses related to access controls. Specifically, we noted the following weaknesses at four locations:

- Although policy was in place to manage service accounts[1] at one location, our test work identified multiple weaknesses related to the management of the accounts. In one instance, we identified an account that had not been removed until our review in May 2018 even though the project utilizing the account had been completed in September 2017. At the same location, we were unable to verify whether five service accounts had been authorized due to the lack of approved authorization forms. In addition, the site inappropriately assigned privileges to the incorrect administrator group. The site also had not reviewed the authorizations, accounts, and privileges of each service account when there was a change to a user's authorization criteria. This resulted in three service account owners continuing to own a service account while they were no longer authorized as administrators.

- Testing at one site identified a weakness related to separation of duties within a financial management system. In particular, a user had write-access within the system that allowed the user to make changes, but the user also had access to allow migration of changes into production. The concept and introduction of separation of duties addresses the potential for abuse of authorized privileges and helps reduce the risk of malicious activity without collusion.

- One location had not fully employed the principle of least privilege to disable an account in a timely manner when such privileges were no longer needed to perform the account user's duties. Specifically, although a user requested one-day temporary use to a specific function within a financial management system in May 2017, the access was not revoked until April 2018.

- Our testing of Web applications at one site identified an application that did not adequately enforce access controls. In particular, users with basic privileges could forcefully browse to Web pages that were supposed to be restricted to privileged users. Once at the restricted pages, the basic privileged user could grant themselves administrative privileges, access data, and execute functions that were reserved for users with higher levels of privileges.

Similar to the issues we identified during our reviews, the Department's Office of Enterprise Assessments also reported on a number of access control vulnerabilities at locations reviewed during FY 2018.

Security and Privacy Training

Our evaluation of the security and privacy awareness practices at the Department identified several weaknesses at three locations. In particular, we found:

[1] A service account is a user account that is created explicitly to provide a security framework for applications running on operating systems. The security framework determines the application's ability to access local and network resources.

- One location had not developed and implemented role-based security training for users with privileged or elevated system access, such as system administrators. The site also had not defined personnel or roles required to take specialized security training nor ensured that such training had occurred.

- Two locations had weaknesses related to ensuring that individuals had met their cybersecurity training requirements as defined by site policy. At one location, 361 of 528 (68 percent) privileged users with security-specific roles had not completed the required training due to a system error. Furthermore, another location had a total of 112 users, including 4 privileged users, who had not completed training in the timeframes required by the site's policy.

- At one site, we found that officials had not ensured that all employees, contractors, and visitors received annual basic privacy training and/or role-based privacy training for personnel having responsibility for personally identifiable information or for activities that involve personally identifiable information. According to Department Order 206.1, *Department of Energy Privacy Program*, individuals must receive yearly training on privacy and data protection policies.

Educating employees on acceptable practices and rules of behavior is critical for both security and privacy awareness programs. A comprehensive and enterprise-wide awareness and training program is paramount to ensuring that people understand their cybersecurity responsibilities, organizational policies, and how to properly use and protect the information technology resources entrusted to them. Furthermore, National Institute of Standards and Technology guidance and the Office of Management and Budget note that all individuals that have been granted access to personally identifiable information must receive appropriate training and, where applicable, specific role-based training.

Security Control Testing

One location reviewed was unable to provide adequate documentation to support that it had tested all appropriate security controls for one of the systems reviewed. According to National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, continuous monitoring is key to ensuring that all system-level security controls (technical, operational, and management controls) are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and continue to be effective over time. However, officials were unable to demonstrate that a complete and thorough assessment had occurred for all required National Institute of Standards and Technology Special Publication 800-53, Revision 4, controls. In particular, we determined that the site could not adequately demonstrate that it tested the majority of required controls for the information system reviewed. During discussions with officials, management indicated that it was unable to document how many controls were tested.

Cybersecurity Program Management

The weaknesses identified occurred, in part, because Department officials had not fully developed and/or implemented policies and procedures related to the issues identified in our report. For instance, similar to previous years, we found that vulnerability and configuration management programs and processes had not ensured that software remained up-to-date and secure. In addition, Department locations had not always implemented effective risk management programs.

Programs and sites had not always developed policies and procedures to ensure fully effective security controls over information systems and data. In particular, we found that a number of locations had not established complete procedures related to areas such as security and privacy awareness training, vulnerability and configuration management, and access controls. For example, our review identified three sites that had not adequately defined training requirements within policies and procedures. One of the sites had not adequately defined privacy requirements within its policies and procedures in accordance with those outlined within Department Order 206.1. In addition, we determined that although one location conducted vulnerability scans, it had not established vulnerability and patch management policies and procedures for the remediation of workstation vulnerabilities. At another location, the vulnerability management procedures were not adequate because they did not account for all known critical and high-risk vulnerabilities as part of the remediation process.

Even when policies and procedures existed, they were not always fully implemented by program and site officials. For example, we identified two sites in which system malfunctions impacted users from obtaining the necessary cybersecurity training. Furthermore, although one location maintained a common controls catalog, it did not require the site to select or document a secure configuration baseline for its databases. In several instances, officials had not ensured that security updates and patches for known vulnerabilities and/or outdated software were applied within timeframes required by site-level policies. Moreover, multiple sites had not established effective processes for either the provisioning, approval, review, or disablement of user accounts, which limited the effectiveness of access control procedures.

In addition to the weaknesses noted above, we determined that at least two locations had not fully implemented effective Web application testing procedures that could have identified and/or mitigated vulnerabilities in a timely manner. In addition, contrary to Federal guidance, one site had not fully tested and documented the effectiveness of all required security controls for the system reviewed. Without an effective security testing process, officials may be unable to maintain an ongoing awareness of information security, vulnerabilities, and threats to support organizational decisions.

Other Cybersecurity Areas of Concern

Phishing and malicious code remain some of the most persistent and pervasive threats to both the Federal Government and the public. These sophisticated attacks take advantage of flaws in software code or use exploits that can circumvent signature-based tools that commonly identify and prevent known threats. Adversaries continue to employ social engineering techniques designed to trick users into opening a malicious Internet link or attachment, thereby giving

attackers unauthorized access to information systems and data. In light of the challenges related to anti-phishing and malware defense and the increasing sophistication of phishing and malicious code attacks, the Department may benefit from adopting additional countermeasure capabilities, such as those identified in Office of Management and Budget Memorandum 17-25, *Reporting Guidance for Executive Order on Strengthening Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017).

As noted in previous reviews, we have identified challenges throughout the Department related to ensuring that cybersecurity policies and procedures are updated in a timely manner to meet Federal requirements. For instance, the Department's primary cybersecurity directive, Department Order 205.1B, *Department of Energy Cyber Security Program*, continues to reference outdated guidance issued by the National Institute of Standards and Technology. We have an outstanding recommendation related to the need to upgrade this policy. In June 2018, the Department's Chief Information Officer issued several Cybersecurity Policy Memoranda related to areas such as anti-phishing, remote access, removable media, and social media. However, it remains to be seen how these memoranda will be implemented by the Department's elements.

The Department continues to experience challenges related to its performance monitoring and plan of action and milestones process. While the plan of action and milestones process is an important tool that assists management in identifying, prioritizing, and tracking remediation activities for known cybersecurity vulnerabilities, we noted that problems remediating plans of action and milestones continued to exist. For example, our review found that 968 of 1,354 (71 percent) open milestones were overdue, including 248 (26 percent) that were overdue by more than 1 year. In at least one instance, we found that a security-related milestone was approximately 6 years past its due date.

Risk to Information Systems and Data

Without improvements to address the weaknesses identified during our evaluation, the Department's information systems and data may be at a higher-than-necessary risk of compromise, loss, and/or modification. The Office of Inspector General continues to recognize cybersecurity as a management challenge area for the Department, emphasizing the critical need to enhance the Department's overall security posture. In addition, we and other independent reviewers continue to identify vulnerabilities related to developing, updating, and/or implementing policies and procedures that may adversely affect the Department's ability to properly secure its information systems and data. Also, without the implementation of effective access controls, the weaknesses noted during our review may increase the risk of unauthorized modification to information systems and the data they contain. Furthermore, without a comprehensive and fully functional security training program, individuals may not fully understand their security responsibilities, organizational policies, and how to properly use and protect the information technology resources entrusted to them. Although locations had implemented compensating controls to mitigate a number of the weaknesses identified during our reviews, our test work found that additional action is necessary to help strengthen the Department's unclassified cybersecurity program.

RECOMMENDATIONS

To correct the weaknesses highlighted in this report, we made 25 recommendations to programs and sites during FY 2018. In particular, we made recommendations to each of the locations where weaknesses were identified related to areas such as vulnerability and configuration management, system integrity of Web applications, access controls, security awareness and privacy training, and security control testing. Corrective actions to address each of the recommendations should be tracked by the Department and, if fully implemented, should help to enhance the Department's unclassified cybersecurity program. In some instances, we also suggested opportunities for improvement at locations reviewed but did not issue them as formal findings and recommendations.

In addition to the recommendations noted above, we recommend that the Administrator for the National Nuclear Security Administration, Under Secretary for Science, Under Secretary of Energy, and relevant staff offices, in coordination with the Chief Information Officer:

1. Ensure appropriate emphasis is placed on correcting identified cybersecurity weaknesses, including addressing findings identified during our current unclassified cybersecurity evaluation. The process should include the effective use of plans of actions and milestones to improve performance monitoring by identifying, prioritizing, and tracking the progress of remediation actions for all identified cybersecurity weaknesses.

MANAGEMENT RESPONSE

Management concurred with the report's recommendation and indicated that corrective actions were planned to address the issues identified in the report. Management also emphasized that the deficiencies identified during our evaluation included ongoing issues that were noted in prior years, including issues related to vulnerability management and management of plans of action and milestones. Furthermore, management commented that known areas of weakness will continue to be addressed at all organizational levels to ensure that the Department's information assets and systems are adequately protected from harm.

OFFICE OF INSPECTOR GENERAL COMMENTS

Management's comments and planned corrective actions were responsive to our recommendation. Management's comments are included in Appendix 3.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

We conducted this evaluation 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 2018 to October 2018 at 27 Department locations primarily under the responsibility of the Administrator for the National Nuclear Security Administration, Under Secretary for Science, and Under Secretary of Energy. Of the 27 locations reviewed, 5 were selected for Office of Inspector General (OIG) 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 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. Our report also considers the results of other reviews conducted by the OIG related to the Department's cybersecurity program. This evaluation was conducted under OIG project number A18TG018.

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, including 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 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, as applicable;

- 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 metric reviews were conducted at five locations across various Department programs/elements; and

- 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.

OIG 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. In utilizing the work of KPMG LLP, we performed procedures that provided a sufficient basis for the use of that work, including obtaining evidence concerning the individual's 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.

Because our review was limited, it would not have necessarily disclosed all internal control weaknesses 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 ensure 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 16, 2018.

RELATED REPORTS

Office of Inspector General

- Special Report on *Management Challenges at the Department of Energy – Fiscal Year 2018* (DOE-OIG-18-09, November 2017). While the fiscal year (FY) 2018 challenge areas remain largely consistent with those in previous years, based on the results of our work over the last year, we have made one notable change. As a result, the FY 2018 management challenges include the following: Contract Oversight, Cybersecurity, Environmental Cleanup, Nuclear Waste Disposal, Safeguards and Security, Stockpile Stewardship, and Infrastructure Modernization.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2017* (DOE-OIG-18-01, October 2017). As noted in the evaluation, the Department of Energy, including the National Nuclear Security Administration, had taken a number of actions to address previously identified weaknesses related to its cybersecurity program. In particular, the Department made progress remediating weaknesses identified in our FY 2016 evaluation, which resulted in the closure of 13 of 16 prior year deficiencies. For instance, the Department reduced the number of vulnerability management findings from nine in FY 2016 to five in FY 2017. While these actions were positive, our evaluation found that the types of weaknesses identified in prior years, including issues related to vulnerability management, system integrity of Web applications, and access controls, continue to exist.

- Audit Report on *The Department of Energy's Implementation of Multifactor Authentication Capabilities* (DOE-OIG-17-08, September 2017). We found that the Department had made progress implementing multifactor authentication; however, additional effort was needed to ensure multifactor authentication was fully implemented across the Department. Specifically, we found that although requirements had existed for more than 10 years, none of the locations reviewed had fully implemented multifactor authentication for secure access to information systems and resources. We also found that multifactor authentication was not always considered for software applications, including those containing sensitive information. Furthermore, information reported by the Department to the Office of Management and Budget was not consistent and did not portray an accurate accounting of its use of multifactor authentication. The issues identified occurred, in part, because Department officials had not adequately planned for the implementation of multifactor authentication on information systems. Specifically, Department guidance and requirements were not always communicated effectively. In addition, the Department had yet to officially approve its multifactor authentication implementation plan. Furthermore, in some instances, contractor representatives noted that multifactor authentication requirements were not noted in site-level contracts and that the implementation lacked adequate funding and technical direction.

- Audit Report on the *Followup on Bonneville Power Administration's Cybersecurity Program* (DOE-OIG-17-06, August 2017). Bonneville Power Administration (Bonneville) made efforts to improve its cybersecurity program since our prior review

such as elevating the Chief Information Officer position for greater visibility, accountability, and oversight. However, we found that Bonneville had not implemented a fully effective cybersecurity program and continued to identify weaknesses in the areas of access controls, vulnerability and configuration management, and contingency planning. Furthermore, we noted that officials had not ensured all systems contained up-to-date security controls. We also noted weaknesses related to risk management. The issues identified occurred, at least in part, because officials had not ensured that Federal and Bonneville requirements were updated and/or fully implemented. For example, contrary to Federal requirements, Bonneville had not implemented an effective continuous monitoring program. Specifically, Bonneville lacked separation of duties related to the individuals that designed security controls and tested those controls. Moreover, Bonneville did not effectively utilize plans of action and milestones, a critical component of an effective continuous monitoring program.

- Special Report on *Management Challenges at the Department of Energy – Fiscal Year 2017* (OIG-SR-17-02, November 2016). The FY 2017 challenge areas remain largely consistent with those in previous years. The FY 2017 management challenges include the following: Financial Assistance and Contract Management, Cybersecurity, Environmental Cleanup, Nuclear Waste Disposal, Safeguards and Security, Stockpile Stewardship, and Infrastructure Modernization.

- Audit Report on the *Management of Brookhaven National Laboratory's Cybersecurity Program* (DOE-OIG-17-02, November 2016). Brookhaven National Laboratory had not implemented a fully effective cybersecurity program. We identified weaknesses related to vulnerability and configuration management, physical and logical access controls, security planning and assessments, and contingency planning and data retention. The identified weaknesses occurred, in part, because Brookhaven National Laboratory officials had not fully implemented applicable requirements related to cybersecurity such as site-specific policies and procedures designed to address many of the areas of weakness noted during our review, including vulnerability management and access controls. We also found that Brookhaven Site Office and laboratory officials had not always effectively monitored the cybersecurity program.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program – 2016* (DOE-OIG-17-01, October 2016). The Department, including the National Nuclear Security Administration, had taken actions 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 weaknesses. 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 evaluation found that the types of weaknesses 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.

- 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 and records management. Based on these findings, we determined that the Energy Information Administration (EIA) had not implemented a fully effective information technology program. In particular, we identified weaknesses related to information technology 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, the EIA had not implemented an effective governance structure over information technology project management and cybersecurity activities. Confusion regarding lines of authority adversely affected EIA's cybersecurity, project management, and records management programs. We noted that weaknesses related to these areas may have been alleviated had the 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, Department 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.

Government Accountability Office

- *HIGH-RISK SERIES: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation* (GAO-18-645T, July 2018)
- *INFORMATION SECURITY: Supply Chain Risks Affecting Federal Agencies* (GAO-18-667T, July 2018)
- *CRITICAL INFRASTRUCTURE PROTECTION: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption* (GAO-18-211, February 2018)
- *FEDERAL INFORMATION SECURITY: Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices* (GAO-17-549, September 2017)
- *INFORMATION TECHNOLOGY: Sustained Management Attention to the Implementation of FITARA Is Needed to Better Manage Acquisitions and Operations* (GAO-17-686T, June 2017)
- *TECHNOLOGY ASSESSMENT: Internet of Things Status and Implications of an Increasingly Connected World* (GAO-17-75, May 2017)
- *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)

MANAGEMENT COMMENTS

EXEC-2018-006460

Department of Energy
Washington, DC 20585

October 11, 2018

MEMORANDUM FOR THE ACTING INSPECTOR GENERAL

FROM: STEPHEN (MAX) EVERETT
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General's Draft Report on "The Department of Energy's Unclassified Cybersecurity Program – 2018"

Thank you for the opportunity to comment on the Draft Evaluation Report, "The Department of Energy's Unclassified Cybersecurity Program - 2018." The Department of Energy (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).

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 management of Plans of Actions and Milestones (POA&Ms). 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 recommendation in this draft report, the Department's response is attached.

If you have any questions or need additional information, please contact Mr. Micah Czigan, Acting Deputy Chief Information Officer for Cybersecurity, at (202) 586-3424.

Attachment

EXEC-2018-006460

MANAGEMENT RESPONSE
IG Draft Report
The Department of Energy's Unclassified Cybersecurity Program – 2018
(Job Code A18TG018)

Recommendation: *Ensure appropriate emphasis is placed on correcting identified cybersecurity weaknesses, including addressing findings identified during our current unclassified cybersecurity evaluation. The process should include the effective use of plans of actions and milestones to improve performance monitoring by identifying, prioritizing, and tracking the progress of remediation actions for all identified cybersecurity weaknesses.*

Response: Concur.

As a result of its reviews, the IG made 25 recommendations to programs and sites during fiscal year (FY) 2018 to improve the Department of Energy's (DOE's) cybersecurity posture. These recommendations have been reviewed at the organizational level, and corrective actions will be identified by the appropriate DOE Program in its Plan of Action and Milestone (POA&M) report, with specific actions and estimated completion dates. Corrective actions will be included in quarterly POA&M reporting to the Office of the Chief Information Officer (OCIO). Additionally, the DOE OCIO will confirm that weaknesses noted in this report are recorded and tracked as POA&Ms. Programs will begin reporting on any open actions related to the recommendations on their first quarter FY 2019 report.

The Program Offices monitor POA&Ms for all subordinate organizations through internal processes that are to be documented in Risk Management Implementation Plans (RMIPs) as required by DOE Order 205.1B, *Department of Energy Cyber Security Program.* 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 execute and refine processes to provide greater consistency and accuracy in reported POA&M data, which includes the Enterprise Cyber Governance System (ECGS), a tool for enterprise POA&M management and reporting. ECGS is now operational and available for all Departmental Elements.

Estimated Completion Date: 09/30/2019

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.