OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

EVALUATION REPORT

DOE-OIG-18-01

October 2017

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2017

Department of Energy
Washington, DC 20585

October 11, 2017

MEMORANDUM FOR THE SECRETARY

FROM: April Stephenson
Acting Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department of Energy's Unclassified Cybersecurity Program – 2017"

BACKGROUND

The Department of Energy operates nearly 100 entities across the Nation and depends on information technology (IT) systems and networks for essential operations required to accomplish its national security, research and development, and environmental management missions. 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. For instance, the Department responded to more than 18,000 potential incidents in fiscal year (FY) 2017 related to areas such as malicious code, information and system compromise, and unauthorized use. Many of these malicious attacks were 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, 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 2017.

RESULTS OF EVALUATION

We found that opportunities existed for the Department to enhance its ability to adequately protect information systems and data. 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, programs and sites made progress remediating weaknesses identified in our FY 2016 evaluation, which resulted in the closure of 13 of 16 prior year weaknesses. 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 current 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. In particular, we found the following:

- Although improvements were made, weaknesses continue to exist related to the Department's vulnerability management program. Specifically, we identified at least three locations that continued to use software on workstations and servers that was missing security patches or was no longer supported by the vendor. We also determined that workstations, laptops, and servers were missing anti-virus software updates designed to protect the information systems. Some of the vulnerability management weaknesses still existed at programs and sites even though they were identified during our FY 2015 and 2016 evaluations.

- Vulnerabilities existed related to system integrity of Web applications. For example, we identified an application at one location that did not adequately prevent malicious input data that, if exploited, could have resulted in unauthorized access to Department resources. Attacks at this location could have allowed an attacker to compromise legitimate users' workstations and application login credentials. In addition, another site had not fully updated and implemented corrective action plans to address previously identified conditions related to system integrity of Web applications.

- Access control weaknesses were identified at six locations. At three locations, we identified user accounts for individuals that were no longer part of the organization. Another location had not enforced identification and verification requirements for privileged users, nor had it implemented appropriate logging capabilities to monitor their activities. Furthermore, even though one site had an established password policy, we identified 223 privileged users who still had system access even after exceeding the established password expiration limitations.

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 current configuration and security patch management processes had not ensured that software remained up-to-date and secure. In addition, the Department had not always implemented effective performance monitoring and risk management programs. For example, we continued to identify concerns with the Department's implementation of plans of action and milestones and the effective use of corrective action plans to address identified weaknesses. We also noted that security testing at several locations reviewed was not fully supportive of an effective continuous monitoring cybersecurity program.

Without improvements to its cybersecurity program in areas such as enhanced controls over vulnerability management and access controls, the Department's systems and information may be at a higher-than-necessary risk of compromise, loss, and/or modification. Furthermore, without improvements to ensure that the most current Federal security requirements are implemented, programs and sites may not keep pace with the challenges facing an ever-changing cybersecurity landscape. Although sites had implemented compensating controls to mitigate weaknesses

identified during our reviews, our test work found that ineffective and untimely vulnerability management and plans of action and milestones processes could potentially allow an attacker to exploit the existing vulnerabilities. In addition, 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. 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 vulnerabilities.

MANAGEMENT RESPONSE

Management concurred with the report's recommendation 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.

Attachment

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

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2017

TABLE OF CONTENTS

Audit Report

Appendices

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2017

BACKGROUND

The *Federal Information Security Modernization Act of 2014* (FISMA) requires the Office of Inspector General (OIG) 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 FISMA evaluation, we conducted extensive control testing and assessments of the unclassified cybersecurity programs at 27 Department locations primarily under the purview of the Administrator for the National Nuclear Security Administration, Acting Under Secretary for Science and Energy, and Acting 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, including test work conducted at five Department locations to support an evaluation against FISMA 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) 2017 evaluation identified that the Department had taken significant action 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 13 of 16 weaknesses reported during our prior year evaluation. For example, the Department made progress in addressing its vulnerability management program by closing six prior year vulnerability findings. 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.

Unclassified Cybersecurity Program

Our FY 2017 evaluation identified weaknesses related to vulnerability management, system integrity of Web applications, and access controls. Although the types of vulnerabilities identified were consistent with our prior evaluations, our FY 2017 review disclosed weaknesses at new locations and noted unresolved weaknesses from the prior year at two locations.

Vulnerability Management

The Department had taken action to address a number of the vulnerability management weaknesses identified in our prior reviews. However, our test work indicated that vulnerability management weaknesses remained – with three prior year findings remaining open and the addition of two 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 risk(s). Our review determined the following:

- At one site, we identified vulnerable database, application, Web, and other network servers running applications that were missing security patches for known vulnerabilities released at least 30 days prior to our testing. Specifically, our review found that 26 of 153 (17 percent) scanned servers were missing security patches released at least 30 days prior to our testing, including servers supporting financial processes. Sixteen of those 26 servers were missing patches identified as critical severity patches and 25 were missing patches identified as high risk. In addition, we determined that nearly 250 workstations, laptops, and/or servers at one site had not received anti-virus software updates.

- Two locations were running applications that the vendor no longer supported. For example, at one site, we identified at least 14 servers operating unsupported software applications related to financial management. We noted that the sites had not appropriately documented and/or accepted the risk of operating the unsupported applications.

- At one site, we found approximately 480 commercial off-the-shelf products missing patches for vulnerabilities rated as critical or high risk, including one device that could have allowed an authenticated attacker to bypass security controls and access higher-privileged functions that are normally restricted to administrative users. Our testing also identified 6 weaknesses that resulted in nearly 1,400 servers being left vulnerable to man-in-the-middle attacks, which allows an attacker to intercept and/or alter communication between 2 parties. Furthermore, we identified one server that had not received vendor support since 2009.

- Officials at one location used a database management tool that the vendor had not supported since July 2010 and an operating system that the vendor had not supported since February 2012. Our test work also found one instance of virus definitions that were more than 8 months old. In addition, our review identified 207 firewall exceptions that were expired but remained open. Several of these exceptions had been expired for more than a year. Although officials were sometimes aware of existing vulnerabilities, documentation justifying risk acceptance for known vulnerabilities contained insufficient detail or did not exist. For example, documentation for one vulnerability did not include any formal acceptance of risk or discussion of mitigating controls.

- Sites also had not fully implemented a vulnerability management program as previously recommended by the OIG. Specifically, one site had not fully implemented corrective action plans to address previously identified conditions related to vulnerability management of network systems and devices. While the site had completed various corrective actions, it had not fully identified and upgraded unsupported software and/or accepted the risk associated with software that was unsupported. Similarly, although another location made progress implementing a process employing mechanisms with regards to malicious code protection, it had not fully addressed all previously identified weaknesses.

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 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 2017.

System Integrity of Web Applications

While the Department had taken action to remediate prior year findings, we identified numerous weaknesses related to system integrity of Web applications at three locations. 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. Specifically, our review found the following:

- Similar to previous findings, we identified Web applications at two locations that 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 allow an attacker to gain unauthorized access to an application, make unauthorized changes to data, and disclose sensitive information. For example, we found one application that lacked formal procedures to validate input parameters for high-risk Web applications prior to acceptance. Specifically, the web application did not validate user input against a set of custom rules to ensure the input met a specific length, type, syntax, or other organizationally defined requirements before accepting the data for further processing.

- We also identified an application that 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.

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

The Department had taken steps to correct access control related weaknesses identified during our prior year review. However, our current evaluation identified several new weaknesses related to access controls. Specifically, we noted the following weaknesses at five locations:

- One site had not uniquely identified and authenticated database administrators. We found that usernames and passwords were shared among database administrators who supported more than 350 databases. In addition, officials at the same location had not fully implemented a database-level logging capability to monitor database administrators' account activities.

- One location had not disabled or removed two unused database administrator accounts in production databases. One account belonged to an active contractor who was no longer

part of the database administrator group and the other account belonged to a terminated employee. When informed of our results, management immediately removed the unused database administrator accounts.

- Testing at one site demonstrated that an application contained three user accounts in a database access listing even though the users were no longer part of the organization. The three accounts remained on the database user listing 36 to 127 days after the account holders' departure dates.

- Although we noted that the policy at one location indicated that passwords for privileged accounts would have a 90-day maximum lifetime limitation, our review found that the site's access listing contained 223 privileged users capable of accessing the system after exceeding the password expiration date. In addition, contrary to its computer access policy and system security plans, we found that the access listing at the same site contained more than 300 outdated accounts, including 22 administrator accounts.

- Applications at one location did not properly enforce access controls. Specifically, despite policies that indicated passwords for non-privileged accounts were set to expire within 180 days, we found the access control listing contained more than 250 accounts that could access applications with expired passwords, including key business applications such as time and attendance and financial management applications.

Access control weaknesses have been an ongoing area of concern for the Department as demonstrated in numerous prior reports issued by the OIG. For instance, our recent report on *Followup on Bonneville Power Administration's Cybersecurity Program* (DOE-OIG-17-06, August 2017) identified both physical and logical access control weaknesses, including not adequately protecting sensitive information such as user credentials (username and password). Similarly, our review of *Management of Brookhaven National Laboratory's Cybersecurity Program* (DOE-OIG-17-02, November 2016) found that data centers were not always adequately secured or that logical access to the site's information systems was appropriately granted. In addition, our recent audit of the *Department of Energy's Implementation of Multifactor Authentication* (DOE-OIG-17-08, September 2017) identified weaknesses related to access controls and personal identity verification (PIV) card implementation, the Federal government's standard for accessing facilities and information systems. 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 six locations reviewed during FY 2017.

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 the configuration and security patch management processes had not ensured that software remained up-to-date and secure. In addition, the Department had not always implemented effective performance monitoring and risk

management programs. For example, we continued to identify concerns with the Department's implementation of plans of action and milestones (POA&M) and the effective use of corrective action plans to address identified weaknesses.

Policies and Procedures

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 vulnerability management, access controls, and system integrity of web applications. At one location, we found that the risk acceptance policies and procedures for known vulnerabilities was not fully documented, a key process in the authorization of information systems. In several instances, we determined that access management policies and procedures related to the implementation of identification and authentication mechanisms had not been developed. One site also had not fully updated and implemented corrective action plans to address previously identified weaknesses related to system integrity of web applications. Furthermore, contrary to Federal requirements, one site had not developed policies or procedures for the use of PIV cards for allowing non-privileged or privileged users access to Federal facilities, networks, and information systems.

Even when policies and procedures were documented, they were not always fully implemented by program and site officials. For example, we identified two sites in which robust patch management processes and procedures had not been implemented to effectively remediate vulnerabilities affecting information system assets. Contrary to existing procedures, officials had not ensured that security updates and patches for known vulnerabilities and/or outdated software were applied in a timely manner. While one site made progress implementing processes to ensure that unsupported software on servers was identified and upgraded to a supported version, the processes had not been fully implemented. Similarly, we determined that officials had not always implemented existing policies and procedures related to access controls. Specifically, officials at several locations had not followed existing access control procedures related to ensuring proper user account access and removal of terminated user accounts.

Performance Monitoring and Risk Management

The Department had not implemented a fully effective performance monitoring and risk management program. The POA&M process is an important tool that assists management in identifying, prioritizing, and tracking remediation activities for known cybersecurity vulnerabilities. However, consistent with prior year evaluations, we noted that progress remediating POA&Ms continued to exist. For example, we found that corrective action plans associated with POA&Ms for three previous findings were not fully implemented, leaving identified weaknesses related to vulnerability management of network systems and devices unmitigated. Our review also found that:

- Since our prior evaluation, the Department had reduced the overall number of milestones, including the number of milestones that were past their estimated completion date. However, our current year analysis determined that 288 of 416 (69 percent) open

milestones were overdue, including 153 (53 percent) that were overdue by more than one year. Last year, we reported that 851 of 1,093 milestones were past the estimated completion date, including 456 that were overdue by more than a year.

- While the total number of weaknesses increased significantly from our prior year evaluation, the number of open weaknesses that were past the scheduled completion date remained consistent. Specifically, we found that total weaknesses increased from 928 in FY 2016 to 1,408 in FY 2017, and total weaknesses past the scheduled completion date increased from 617 in FY 2016 to 620 in FY 2017. Our review also found that total weaknesses past due by more than one year decreased slightly from 387 in FY 2016 to 376 in FY 2017.

Management commented that it is within management's authorities to prioritize work and resources along with risk impact. While we agree that those are part of management's responsibilities, we remain concerned with the limited progress made by the Department reducing the number of cybersecurity weaknesses in a timely manner.

Consistent with our prior year evaluation, we also determined that appropriate risk management practices, including a continuous monitoring program, were not always effectively implemented at the programs and sites reviewed. For example, we noted at least two locations had not fully implemented effective Web application testing procedures that could have identified and mitigated vulnerabilities in a timely manner. One location had not yet completed corrective actions to ensure that high and medium risks in Web applications were identified, analyzed, and reviewed for remediation and/or risk acceptance. Another location had not fully implemented a Web application testing process to ensure that all vulnerabilities were identified and remediated in a timely manner. Furthermore, we found that one site had not fully tested the effectiveness of security controls on various systems reviewed. An effective continuous monitoring process should help officials maintain an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Other Cybersecurity Areas of Concern

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. 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 issued by the National Institute of Standards and Technology. Specifically, rather than reference National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, which was issued in April 2013, it references the prior version that was issued in April 2009. National Institute of Standards and Technology recently released a draft of Special Publication 800-53, Revision 5, and anticipates publishing the final version no later than December 2017. Considering the Department's challenges with implementing existing guidance and the impending release of new requirements, we are particularly concerned that the Department is in danger of falling even further behind on its implementation of updated cybersecurity policies and procedures.

Phishing and malicious code are some of the most persistent and pervasive threats to both the Federal government and the public at large. These increasingly 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. Increasingly, adversaries 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. The Office of Management and Budget's *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2016* (March 10, 2017) indicated that the Department reported 99 incidents pertaining to email/phishing, one of the highest attack vectors facing the Department. Given the Department's previous struggles with meeting FISMA goals 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 19, 2017).

We also identified an ongoing challenge related to the Department's implementation of multifactor authentication, specifically the use of PIV cards. We found that the Department made significant improvements in its implementation of PIV cards at the network level for privileged and standard users, increasing the number of users utilizing PIV cards from approximately 12 percent to approximately 73 percent as of June 2017. While officials estimate that they will meet the current Office of Management and Budget requirements for network access by January 2018, several challenges still exist related to fully implementing PIV cards. Specifically, the Department will need to address PIV card implementation for local, remote, and application access once it has completed network access to fully comply with Office of Management and Budget requirements for implementing PIV cards as the standard for accessing Federal information systems. We recently issued a separate report for our audit on the *Department of Energy's Implementation of Multifactor Authentication Capabilities*.

Risk to Information and Systems

Without 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 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. In addition, the OIG 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. Furthermore, 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. Although sites had implemented compensating controls to mitigate a number of the weaknesses identified during our reviews, our test work found that ineffective and untimely vulnerability management and POA&M processes could potentially allow an attacker to exploit the existing vulnerabilities. Therefore, additional action is necessary to help strengthen the Department's unclassified cybersecurity program.

RECOMMENDATIONS

To correct the weaknesses highlighted in this report, we made 30 recommendations to programs and sites during FY 2017, including 5 recommendations related to prior year weaknesses, designed to improve the Department's cybersecurity posture. 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, policies and procedures, and continuous monitoring. 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 addition to the recommendations noted above, we recommend that the Administrator for the National Nuclear Security Administration, Acting Under Secretary for Science and Energy, and Acting Under Secretary for Management and Performance, in coordination with the Chief Information Officer, direct Federal and contractor programs and sites to:

1. Ensure appropriate emphasis is placed on correcting identified cybersecurity weaknesses, including addressing findings identified during our prior unclassified cybersecurity evaluations. The process should include the effective use of POA&Ms 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 had been initiated or 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. 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.

AUDITOR 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

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 2017 to October 2017 at 27 Department locations primarily under the responsibility of the Administrator for the National Nuclear Security Administration, Acting Under Secretary for Science and Energy, and Acting Under Secretary for Management and Performance. Of the 27 locations, 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 A17TG020.

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

- 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 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.

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 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 officials waived an exit conference on October 10, 2017.

RELATED REPORTS

Office of Inspector General

- Audit Report on *The Department of Energy's Implementation of Multifactor Authentication Capabilities* (DOE-OIG-17-08, September 2017). We found that the Department of Energy had made progress in 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). While the fiscal year (FY) 2017 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 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 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 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 current 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.

- Evaluation Report on *The Department of Energy's Unclassified Cybersecurity Program - 2015* (DOE-OIG-16-01, November 2015). The Department had taken positive steps over the past year to address previously identified cybersecurity weaknesses related to its unclassified cybersecurity program. Specifically, we noted that the Department made significant progress in remediating weaknesses identified in our FY 2014 evaluation, which resulted in the closure of 22 of 26 reported weaknesses. While these actions were positive, our evaluation found that the types of weaknesses 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 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 and records management. Based on these findings, we determined that the Energy Information Administration 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 Energy Information Administration management had not ensured that applicable Federal and Department policies and procedures were always implemented. Furthermore, the Energy Information Administration had not implemented an effective governance structure over information technology project management and cybersecurity activities. Confusion regarding lines of authority adversely affected the Energy Information Administration's cybersecurity, project management, and records management programs. We noted that weaknesses related to these areas may have been alleviated had the Energy Information Administration 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.

Government Accountability Office

- *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)

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

- *CYBERSECURITY: Actions Needed to Address Challenges Facing Federal Systems* (GAO-15-573T, April 2015)

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

October 4, 2017

MEMORANDUM FOR APRIL STEPHENSON
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 – 2017"

Thank you for the opportunity to comment on the Draft Evaluation Report, "The Department of Energy's Unclassified Cybersecurity Program - 2017." 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 enclosed.

If you have any questions or need additional information, please contact Mr. Mark Jarek, Deputy Chief Information Officer for Cybersecurity, at 202-586-6060.

Sincerely,

Stephen (Max) Everett
Chief Information Officer

Printed with soy ink on recycled paper

Enclosures

Enclosure 1

MANAGEMENT RESPONSE
IG Draft Report
The Department of Energy's Unclassified Cybersecurity Program – 2017
(Job Code A17TG020)

Recommendation: *Ensure appropriate emphasis is placed on correcting identified cybersecurity weaknesses, including addressing findings identified during our prior unclassified cybersecurity evaluations. The process should include the effective use of POA&Ms 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 30 recommendations to programs and sites during fiscal year (FY) 2017 to improve the Department'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 2018 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: 09/30/2018

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.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu