OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

EVALUATION REPORT

DOE-OIG-20-12

November 2019

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM - 2019

Department of Energy
Washington, DC 20585

November 19, 2019

MEMORANDUM FOR THE SECRETARY

FROM: Teri L. Donaldson
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department of Energy's Unclassified Cybersecurity Program – 2019"

BACKGROUND

The Department of Energy operates many facilities across the Nation that depend on information technology systems and networks for essential operations required to accomplish national security, research and development, and environmental management missions. As information technology continues to evolve, there are greater opportunities for efficiencies and accessibility to information but also increased cybersecurity threats. To supplement existing requirements, the *National Cyber Strategy* was released in September 2018 to help protect public and private systems and information. While the Office of Management and Budget recently reported that the number of incidents agencies reported decreased, the systems used to support the Department's various missions continue to face millions of cyber threats each year ranging from unsophisticated hackers to advanced persistent threats using state-of-the-art intrusion tools and techniques.

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 fiscal year 2019.

RESULTS OF EVALUATION

We determined that opportunities existed for the Department, including the National Nuclear Security Administration, to improve the protection of unclassified 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 2018 evaluation, which resulted in the closure of 21 of 25 (84 percent) prior year recommendations. Although these actions were positive, our current

evaluation identified weaknesses that were consistent with our prior reports related to vulnerability management, configuration management, system integrity of Web applications, access controls and segregation of duties, cybersecurity and privacy training, and security control testing and continuous monitoring. In particular, we found the following:

- Eleven sites reviewed had critical and/or high-risk vulnerabilities on the workstations and servers tested. For example, we noted that more than half of the 1,848 workstations tested were operating with missing patches and/or updates that had been released at least 30 days prior to our testing. At 1 location, we determined that there were nearly 11,000 critical and high-risk vulnerabilities related to missing security patches or software no longer supported by the vendor on the 159 workstations included in our sample. In addition, two locations included in our prior year review had not fully addressed recommendations related to vulnerability management weaknesses as neither site had completed all corrective action plan milestones.

- Configuration management weaknesses existed at three sites. For instance, firewall rules at one location were not configured properly and allowed certain systems connected to the general support network to inappropriately access another network supporting an industrial control system at the site. At another location, we found that officials had not developed a configuration management plan, and security baseline configurations were not consistently implemented. The use of secure configurations that emphasize hardening of systems against flaws can result in greater levels of security and protection from future vulnerabilities.

- Weaknesses related to system integrity of Web applications were identified at four locations. The weaknesses included 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.

- Although the Department had corrected previously identified weaknesses, access control and segregation of duties issues existed at six locations. For instance, our test work uncovered weaknesses related to access controls over peripheral devices such as printers/multifunction devices, management of privileged and non-privileged user accounts, and timely reviews of user accounts over a financial management system.

- Weaknesses existed related to the Department's cybersecurity and privacy training at two locations. In particular, two sites had not developed and implemented role-based training strategies/plans for all appropriate personnel. In addition, officials had not ensured that adequate privacy awareness training was provided annually for all employees at one location.

- Significant deficiencies related to security control testing and continuous monitoring were identified at two locations. For instance, although a corrective action plan was in place and in the process of being implemented, one location was unable to provide adequate documentation to support that it had processes for ongoing assessments, granting system

authorizations, or monitoring security controls. At another location, we determined that the site's control testing and monitoring process was neither complete nor effective. For example, we found that site officials did not test controls for significant systems to ensure that they existed and were operating as intended.

The weaknesses identified in our report occurred due to a variety of reasons. For instance, we noted that vulnerability management weaknesses existed at one location because officials only conducted technical scanning for vulnerabilities on an ad-hoc basis, and the site did not have a process to regularly conduct vulnerability scanning of the entire environment. In some instances, software management tools and processes did not ensure that software was upgraded prior to the end-of-support dates. Furthermore, we found that Web applications remained vulnerable because sites did not always ensure that appropriate safeguards were in place and operating effectively. For example, certain locations tested had not always developed and implemented adequate testing processes and procedures to identify vulnerabilities related to data confidentiality and integrity of authentication functionality in Web applications.

Throughout fiscal year 2019, we made 54 recommendations to programs and sites related to improving the Department's cybersecurity program. Furthermore, in some instances, we provided opportunities for improvement at locations reviewed but did not issue formal recommendations. 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 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. Therefore, additional action is necessary to help strengthen the Department's unclassified 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 recommendations made throughout the evaluation and indicated that corrective actions were taken or 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
Chief Information Officer
Administrator, National Nuclear Security Administration
Administrator, Energy Information Administration
Deputy Chief Financial Officer

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2019

TABLE OF CONTENTS

Evaluation Report

Appendices

THE DEPARTMENT OF ENERGY'S UNCLASSIFIED CYBERSECURITY PROGRAM – 2019

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 28 Department locations primarily under the purview of the National Nuclear Security Administration, Under Secretary for Science, Under Secretary of Energy, and certain 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 and prior 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 of Energy's Office of Enterprise Assessments when reporting on the Department's cybersecurity program.

Our fiscal year (FY) 2019 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 21 recommendations made 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 at 28 locations during FY 2019 revealed that the majority of identified vulnerabilities were similar in type to those identified during prior evaluations.

DETAILS OF FINDINGS

Our FY 2019 evaluation identified weaknesses related to vulnerability management, configuration management, system integrity of Web applications, access controls and segregation of duties, cybersecurity and privacy training, and security control testing and continuous monitoring. Although the types of vulnerabilities identified were mostly consistent with our prior evaluations, our FY 2019 review disclosed weaknesses at a number of new locations. Our test work specific to the FY 2019 evaluation resulted in 34 new and 4 repeat recommendations at 9 locations.

Vulnerability Management

The Department had taken action to address many of the vulnerability management weaknesses identified in our prior review. However, recommendations related to vulnerability management at two prior year locations remained open. Both locations continued to operate systems without

current security patches for known vulnerabilities. Similarly, this year, we also identified vulnerability management weaknesses at 11 sites. Vulnerability management is the process of identifying, evaluating, and either mitigating or formally accepting the risks. Our review determined the following:

- Eleven sites were running unsupported software on network servers and/or workstations. For example, our limited testing at 1 site found critical and high-risk vulnerabilities related to unsupported software on 5 of 10 servers tested. Furthermore, 9 sites reviewed had unsupported software running on workstations, including 1 site where we found 365 critical and high-risk vulnerabilities present on 118 of 159 (74 percent) workstations tested. At another location, we identified that nearly every workstation tested contained critical and high-risk vulnerabilities related to unsupported software.

- Nine locations were operating workstations and servers that had missing critical and high-risk vulnerability security patches and/or updates. In particular, we found that 1,004 of 1,848 (54 percent) workstations tested were operating with missing patches and/or updates that had been released at least 30 days prior to our testing. At 1 location, we determined that all 416 workstations tested had missing patches to address critical and high-risk vulnerabilities. At another site, we found over 10,500 critical and high-risk vulnerabilities related to missing updates and patches on the 159 workstations tested. Similarly, we also determined that 142 of 297 (48 percent) servers tested were missing critical or high-risk patches and/or updates, including all servers tested at 2 locations.

- One location had workstations with outdated antivirus definitions or workstations with antivirus services not running correctly. Specifically, the antivirus application applied to remote hosts had not been installed successfully. Although we noted that there was only a small number of workstations affected by the vulnerability, the issue presented risk to the office's systems and data. Notably, officials had developed a plan of action and milestones to resolve the weakness.

The vulnerability management weaknesses at the reviewed sites occurred for a number of reasons. For instance, although one site had deployed an automated scanning tool for its workstations and servers, the scanning occurred on an ad-hoc basis, and the site did not have a process to conduct vulnerability scanning of the entire environment on a regular basis. In addition, software management tools and processes did not ensure that software was upgraded prior to the end-of-support dates. Furthermore, prior year weaknesses continued to exist at two locations because officials had not yet completed corrective action plans to address known vulnerability management issues. Without effective vulnerability management practices, applications that are missing security patches for known vulnerabilities are at risk for computer viruses and other malicious attacks that could give attackers control of the applications or even an entire server.

We concluded that all locations reviewed 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 operations. In addition to our test work, the Department's Office of Enterprise Assessments reported on vulnerability management weaknesses and opportunities for improvement at numerous sites during FY 2019.

Configuration Management

The Department had taken action to address one of the configuration management weaknesses identified in our prior review. However, our test work indicated that configuration management weaknesses continued to exist, with one prior year finding remaining open and the addition of two new findings. Configuration management is the collection of activities focused on establishing and maintaining the integrity of information systems. For the cybersecurity environment, an effective configuration management process ensures that required adjustments to system configurations do not adversely affect the security of the information system or organization. Our review determined the following:

- During a review of firewall rules at one site, we determined that the rules allowed certain systems connected to the general support network to inappropriately access two Web servers on another network supporting a primary industrial control system at the site. In addition, multiple firewall rules allowed specific systems and/or internet protocol ranges to connect to other systems on different networks. Without an effective firewall rule review process, unauthorized rule changes may not be detected and could potentially allow unauthorized access to restricted resources.

- At one location, a shared file destination was configured to allow anonymous access. As such, anyone with network access to the general support system could have connected to the shared drives/files without credentials and inappropriately accessed files. Failure to remediate these conditions could result in additional systems or components with unknown and undetected security vulnerabilities being introduced into and remaining in the production environment.

- Our evaluation also identified a weakness related to the management of baseline configurations at one site. As part of a holistic risk management strategy that applies the information security concept of defense-in-depth, organizations are required to employ appropriate configuration settings for organizational systems. However, we determined that the site did not have a configuration management plan, and although procedures for developing security baselines were generally defined, they were not consistently implemented. 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. Notably, this issue was included in the site's cybersecurity program corrective action plan.

The identified weaknesses related to configuration management at one location occurred, in part, because site officials had not established a process to periodically review the effectiveness and configuration of proposed firewall rules. In addition, we determined that another site's

vulnerability and configuration management processes did not ensure that systems with anonymous access, default credentials, or vulnerable protocols were identified, monitored, and remediated.

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 four locations. In particular, we identified the following deficiencies:

- Web applications at two locations did not properly validate input data and/or protect the confidentiality of user credentials. Specifically, the applications could have accepted malicious input data that could have been used to launch attacks against legitimate application users, resulting in unauthorized access to the applications. During our prior year review, similar weaknesses were identified at one of the same locations.

- A financial management application at one location used an insecure setting that increased the exposure of user authentication session tokens and the risk that a valid user session could have been compromised. At the same location, two applications were accessible over a clear-text protocol – meaning that an attacker eavesdropping on the network could have obtained sensitive information transmitted between users and the application, including usernames and passwords.

- At another location, a Web application used to manage foreign assignments and visits did not enforce access controls for most of its functionality and pages. As a result, any authenticated user with application authorization could have inappropriately obtained access to all data available in the application and used all functions by directly browsing to the desired content. The same application also could have accepted malicious input data from authenticated users that could be used to view, modify, or delete data stored in the database.

The identified weaknesses related to system integrity of Web applications generally occurred because Web application session management was configured without ensuring that adequate data confidentiality safeguards were in place and operating effectively. In addition, vulnerability management programs at the sites reviewed did not always include adequate Web application testing processes and procedures to identify vulnerabilities related to data confidentiality and integrity of authentication functionality in Web applications. 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

Access controls determine the allowed activities of legitimate users and mediate every attempt by a user to access a resource in the system. Although the Department corrected each of the access

control related weaknesses identified during our prior year review, our current evaluation identified new weaknesses related to access controls at six locations. For instance:

- Two sites had not always implemented adequate cybersecurity access controls over peripheral devices. Specifically, we identified access control weaknesses related to printers/multifunction devices, networking devices, and Voice over Internet Protocol devices within business systems and badging/local police systems. We noted devices with default credentials and open configurations that did not require any credentials for access. For example, at 1 location, we found 14 printer/multifunction devices with default credentials and 47 printer/multifunction devices with open configurations that did not require any credentials to be accessed. Using weaknesses identified while testing the devices, we also confirmed the ability to forward scanned and faxed documents to an external email address on printer/multifunction devices.

- Testing at one location identified weaknesses related to segregation of duties. In particular, server system administrators had not segregated the use of privileged and non-privileged accounts. This increased the risk of inappropriate access or unauthorized changes to financial data. In addition, tests of a primary financial business application at the site determined that individuals were inappropriately assigned conflicting roles and responsibilities such as database administration and project billing roles. The concept and introduction of segregation of duties addresses the potential for abuse of authorized privileges and helps reduce the risk of malicious activity without collusion.

- Although one site's system security plan had specific language for the assignment of privileged and non-privileged accounts, our test work identified two non-privileged user accounts that were assigned privileged roles to a database. The data in the database was used for financial reporting for environmental management systems and other business applications. We determined that this weakness in database account management could have resulted in non-privileged users executing privileged functions on the database and increased the risk of modification of the financial data.

- One location had various weaknesses related to access controls and segregation of duties. For instance, site officials had not conducted required quarterly reviews of user accounts and their assigned responsibilities in the site's financial system. Untimely management review of the user accounts and responsibilities may increase the risk of inappropriate access to financial data. At this same location, testing disclosed that the site had not always segregated the use of privileged and non-privileged accounts for system administrators. Furthermore, the site had not implemented multifactor-authentication for certain privileged users or ensured that password requirements for privileged and service accounts were enforced.

The identified weaknesses related to access controls 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 access control programs and processes had not ensured that protective measures, such as segregation of duties,

were enforced through the use of role-based access controls. Reviewing accounts to validate continued access and compliance with account management policy can help ensure the confidentiality, integrity, and availability of systems. In addition, certain locations had not developed and implemented standard operating procedures to ensure that all peripheral devices were configured properly and default credentials were changed upon installation prior to connection to the site's network. 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 2019.

Cybersecurity and Privacy Training

Our evaluation of the cybersecurity and privacy training practices at select Department locations identified weaknesses at two sites. In particular, we found:

- One site had not fully developed a role-based cybersecurity training program for cybersecurity professionals. Specifically, at one site, officials had not defined processes for ensuring that all personnel with significant security roles and responsibilities were provided specialized security training prior to gaining information system access or performing assigned duties periodically thereafter. Notably, the site had a corrective action plan in place to address the issue at the time of our review.

- Two sites had not provided role-based training for individuals having responsibility for managing personally identifiable information or for activities that involve personally identifiable information. Federal guidance requires targeted role-based privacy training for persons in these roles. In addition, one site did not ensure that adequate privacy awareness training was provided annually for all employees.

The identified conditions occurred, in part, because site officials had not ensured that cybersecurity and privacy training policies were developed and implemented. For instance, we noted that one site had not adequately defined training requirements within policies and procedures. In addition, two sites had not adequately defined privacy requirements within their policies and procedures in accordance with those outlined within Department Order 206.1, *Department of Energy Privacy Program*.

Security Control Testing and Continuous Monitoring

We identified significant weaknesses related to security control testing and continuous monitoring at two locations. For instance, one location was unable to provide adequate documentation to support that it had processes for ongoing assessments, granting system authorizations, or monitoring security controls. The same site also did not have effective policies and procedures for conducting system-level risk assessments related to identifying and prioritizing internal and external threats and security controls to mitigate risks. Notably, the site had developed and was in the process of implementing corrective actions related to its cybersecurity program, including continuous monitoring and risk management. At another location, we determined that the site's control testing and monitoring process was neither complete nor effective. For example, we

found that site officials did not test controls for significant systems to ensure that the controls existed and were operating as intended. When weaknesses were identified, they were not always included in a plan of actions and milestones to monitor the status of corrective actions.

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. Furthermore, without an effective risk management process, officials may be unable to maintain an ongoing awareness of information security, vulnerabilities, and threats to support organizational decisions.

Risk to Information and Systems

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. As with previous years, 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. For instance, phishing and malicious code remain some of the most persistent and pervasive threats to both the Federal Government and the public. 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. During FY 2019, our phishing campaign at 1 location found that 78 of 1,230 (6 percent) unique email accounts submitted a phishing form from the malicious link that was created during our testing.

Furthermore, 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. Absent a comprehensive and fully functional cybersecurity training program, individuals also may not fully understand their security responsibilities and organizational policies or 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. Notably, the Department recently revised and issued its primary cybersecurity directive, Department Order 205.1C, *Department of Energy Cybersecurity Program*. The Department's Office of the Chief Information Officer also 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 the directive and memoranda will be implemented by the Department's elements.

RECOMMENDATIONS

To correct the cybersecurity weaknesses identified throughout the Department, we made 54 recommendations to programs and sites during FY 2019 to include this evaluation and other issued reports. Specifically, during this evaluation, we made recommendations to each of the locations where identified weaknesses were related to areas such as vulnerability management, configuration management, system integrity of Web applications, and access controls and segregation of duties. 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 provided opportunities for improvement at locations reviewed but did not issue them as formal findings and recommendations. In addition, other reports we issued in FY 2019 were related to areas such as security over industrial control systems at selected locations and management of the Department's legacy information technology infrastructure. These reports also included recommendations for improving the Department's cybersecurity posture.

MANAGEMENT RESPONSE

The Department concurred with the 54 recommendations issued this year to Department programs and sites related to improving the Department's cybersecurity program. Management noted that this evaluation identified deficiencies in prior years, including ongoing issues related to vulnerability management, configuration management, system integrity of Web applications, access controls and segregation of duties, cybersecurity and privacy training, and security control testing and continuous monitoring. Management indicated that the Department will continue to address each of these weaknesses at all the organizational levels to adequately protect the Department's information assets and systems from harm.

Management's comments are included in Appendix 3.

OFFICE OF INSPECTOR GENERAL COMMENTS

Management's comments and planned corrective actions were responsive to recommendations made during our evaluation.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

We conducted this evaluation to determine whether the Department of Energy's unclassified cybersecurity program protected data and information systems in accordance with Federal and Department requirements.

Scope

We conducted the evaluation from February 2019 to October 2019 at 28 Department locations primarily under the responsibility of the Administrator for the National Nuclear Security Administration, Under Secretary for Science, Under Secretary of Energy, and certain staff offices. Of the 28 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 of Energy'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 A19TG013.

Methodology

To accomplish our objective, we:

- Reviewed Federal regulations and Department directives pertaining to information security 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 selected Department programs and 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 of Energy programs/elements.

- 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. To assess 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 onsite personnel and performed other procedures to satisfy ourselves as to the reliability and sufficiency 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 November 1, 2019.

RELATED REPORTS

Office of Inspector General

- Management Alert on *Management of Cybersecurity Activities at a Department of Energy Site* (DOE-OIG-19-44, August 2019). The Office of Inspector General initiated a review of the cybersecurity program at a selected Department of Energy site in January 2019. Preliminary results of test work conducted at the site revealed potentially significant cybersecurity vulnerabilities on the site's general support system and missing or deficient cybersecurity practices, including the lack of most components of a Risk Management Framework. Due to the nature of the work conducted at the site and the use of systems that had mission critical and safety significant functions, we issued this management alert to ensure management was provided the opportunity to initiate immediate actions to address risks identified within the site's cybersecurity program.

- Audit Report on *Management of a Department of Energy Site Cybersecurity Program* (DOE-OIG-19-42, July 2019). We found that the site had not fully implemented its cybersecurity program in accordance with Federal and Department requirements. We identified weaknesses related to vulnerability and configuration management, logical and physical access controls, contingency planning, and continuous monitoring. As a result, the integrity, confidentiality, and availability of systems and data managed by the site may be impacted by the vulnerabilities identified during our review.

- Audit Report on *Security Over Industrial Control Systems at Select Department of Energy Locations* (DOE-OIG-19-34, June 2019). We found that while the Department continued to make improvements related to its cybersecurity program, additional efforts were needed to ensure that security controls were implemented to protect industrial control systems. Specifically, at various locations, we found issues with security control documentation, vulnerability management, and access controls. In addition, we found locations that had not always developed complete inventories of industrial control systems.

- Special Report on *Management Challenges at the Department of Energy – Fiscal Year 2019* (DOE-OIG-19-07, November 2018). Similar to previous reports concerning the Department's challenge areas, the challenges identified for fiscal year (FY) 2019 remained largely consistent with previous years. These challenges included 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 – 2018* (DOE-OIG-19-01, October 2018). The Department, including the National Nuclear Security Administration, had taken actions to address previously identified weaknesses related to its cybersecurity program. In particular, programs

and sites made progress remediating weaknesses identified in our FY 2017 evaluation, which resulted in the closure of all 12 prior year weaknesses. Although these actions were positive, our 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. We also identified both phishing and malicious code as some of the most persistent and pervasive threats to both the Federal Government and the public.

- 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 that 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.

- Audit Report on the *Follow-up on Bonneville Power Administration's Cybersecurity Program* (DOE-OIG-17-06, August 2017). Bonneville Power Administration 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 Power Administration 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 that all systems contained up-to-date security controls. We also noted weaknesses related to risk management.

Government Accountability Office

- *INFORMATION SECURITY: Supply Chain Risks Affecting Federal Agencies* (GAO-18-667T, July 2018)
- *HIGH-RISK SERIES: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation* (GAO-18-645T, 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)

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

October 31, 2019

MEMORANDUM FOR TERI L. DONALDSON
INSPECTOR GENERAL

FROM: ROCKY CAMPIONE
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General's Draft Report on "The Department of Energy's Unclassified Cybersecurity Program – 2019"

The Department of Energy (DOE or Department) appreciates the opportunity to comment on the Office of Inspector General's (IG) Draft Evaluation Report titled, "*The Department of Energy's Unclassified Cybersecurity Program - 2019.*" 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 IG.

The Department concurs with the 54 recommendations issued this year to DOE's programs and sites related to improving the Department's cybersecurity program.

The IG's assessment identified deficiencies noted in prior years, including ongoing issues related to vulnerability management, configuration management, system integrity of Web applications, access controls and segregation of duties, cybersecurity and privacy training, and security control testing and continuous monitoring. The Department will continue to address each of these weaknesses at all the organizational levels to adequately protect DOE's information assets and systems from harm..

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

Sincerely,

Rocky Campione
Chief Information Officer

Printed with soy ink on recycled paper

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) 586-1818. For media-related inquiries, please call (202) 586-7406.